Gmail

Jon F Turpin <jt4590@gmail.com>

A new FLASH titled "Indicators of Attempted Network Compromise Through Endpoint Device Using Malicious Cobalt Strike" has been posted to the InfraGard system.

1 message

infragardteam@ignconnect.org <infragardteam@ignconnect.org> Fri, Oct 15, 2021 at 7:04 AM
To: jt4590@gmail.com

Attention InfraGard member,

You have received a new broadcast message.

A new FLASH titled "Indicators of Attempted Network Compromise Through Endpoint Device Using Malicious Cobalt Strike" has been posted to the InfraGard system.

To read this document you must login to the InfraGard system. This document is located on the secure site: Publications > Documents > Flash & Pins.

Please contact InfraGardTeam@fbi.gov for account assistance.

Please do not reply directly to this email. Thank you!

On Aug 24, 2023, 9:50 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:
I understand that our Honorable Jim Jordan is requesting any information relating to the federal government in DA Fani Willis' investigation...

The whole thing is Federal because it's dealing with federal election votes and potentially fraud tying counties together between states with similar county names.

Look at Wayne County and how many states it's within, the at Fulton County, then Santa Cruz County, in Arizona ties to California...

Do you know how simple it would be to copy and/or change the data in a SQL database if it got hacked in any voting machines if they had any external internet connection or even if someone plugged in a Bluetooth dongle if they knew what operating system it was on?

Or even less trackable, if someone were to open the SQL database without changing it or even the timestamps on the hard drives, if these were sent somewhere and bad apples were inclined to do so to change the votes?

It's not like changing a traditional file and having the timestamp be changed to reflect the update. It could be done via temp tables without changing the underlying database, then sent to printers to print paper ballots.

Then, someone could simply not save the underlying changes to the database, leaving paper ballots as the only evidence of fraud.

To my knowledge we don't have the same security features on paper ballots that we even have in our paper money to ensure they aren't counterfeit, and we haven't started using the blockchain with encryption with its public ledger to perform vote counting yet.

Of course, we see how cyber criminals even break that system of credibility with "DeFi" cryptocurrency by hiding the ledger in an e change and changing the "smart contracts."

I digress, the point here is that the paper ballots could easily be forged and used to cause a statistically significant impact at the county levels, but a statistically insignificant percentage of votes at the state levels, to win an election in swing states, in a way that is however overall so improbable at the big picture level that it finally raises eyebrows.

Especially when there's a pattern like this. The whole thing is federal, at the very least, and it absolutely is a U.N. mayter as well, and Zimbabwe, in my opinion, actually did the correct thing, and our Honorable Jessica Jennings may need to retract her USAID statement until further investigation may be performed. If Zimbabwe is willing to work with the core U.N. Intelligence agencies and cooperate to research this in depth they're trying to figure this out and aren't the issue.

This is "why" Zimbabwe may be stopping the counts because the issue is that even if you recount, unless you can identify which if any ballots are fake, you don't spot the problem.

I saw this as a possibility when I sent a donation to Zimbabwe a short while ago.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice
-------- Original Message --------
On Aug 24, 2023, 7:28 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:

IN MY OPINION,
THE COUNTIES AT BORDER CROSSINGS WOULD BE THE MAIN TARGETS, AND THE REASON LOUISIANA HAS AVOIDED THIS ISSUE IS BECAUSE OF HAVING PARISHES. IT'S A BIT DIFFERENT TO HAVE PARISHES VS. COUNTIES AND IT WOULD MAKE IT A BIT HARDER FOR BAD APPLES TO BE FORGING BALLOTS AGAINST LOUISIANA USING THE METHOD WHICH I'M IDENTIFYING AS POSSIBLE IN THIS SITUATION.

WAYNE COUNTY IN MICHIGAN HOLDS DETROIT AND A BORDER CROSSING.

Wayne County

18 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

Wayne County may refer to:

Counties in the United States [edit]

- Wayne County, Georgia
- Wayne County, Illinois
- Wayne County, Indiana
- Wayne County, Iowa
- Wayne County, Kentucky
- Wayne County, Michigan
- Wayne County, Mississippi
- Wayne County, Missouri
- Wayne County, Nebraska
- Wayne County, New York
- Wayne County, North Carolina
- Wayne County, Ohio
- Wayne County, Pennsylvania
- Wayne County, Tennessee
- Wayne County, Utah
- Wayne County, West Virginia

FULTON COUNTY EXISTS IN MOST OF THE STATES IN OUR CENTER LOGISTICS.

Fulton County

29 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

Fulton County is the name of eight counties in the United States of America. Most are named for Robert Fulton, inventor of the first practical steamboat:

- Fulton County, Arkansas, named after Governor William Savin Fulton
- Fulton County, Georgia, the most populous of Georgia's counties and by far the most populous county bearing the name
- Fulton County, Illinois
- Fulton County, Indiana
- Fulton County, Kentucky
- Fulton County, New York
- Fulton County, Ohio
- Fulton County, Pennsylvania

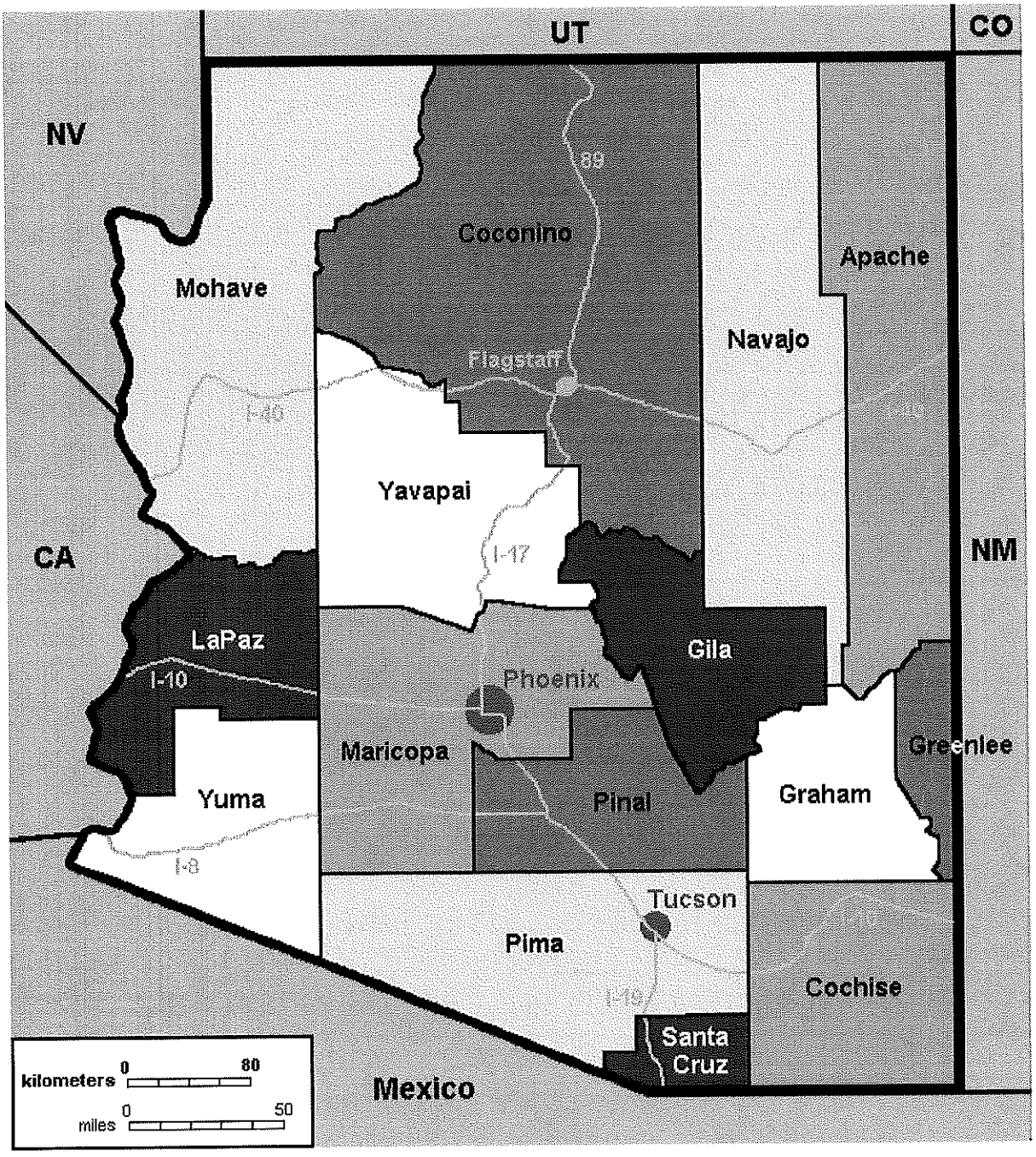
Other uses [edit]

- *Fulton County* (novel) by James Goldman
- Atlanta–Fulton County Stadium, former home to the Atlanta Braves (1966–96) and the Atlanta Falcons (1966–91)

*This disambiguation page lists articles associated with the title **Fulton County**.*
If an internal link led you here, you may wish to change the link to point directly to the intended article.

Categories: Disambiguation pages | Place name disambiguation pages | United States county name disambiguation pages

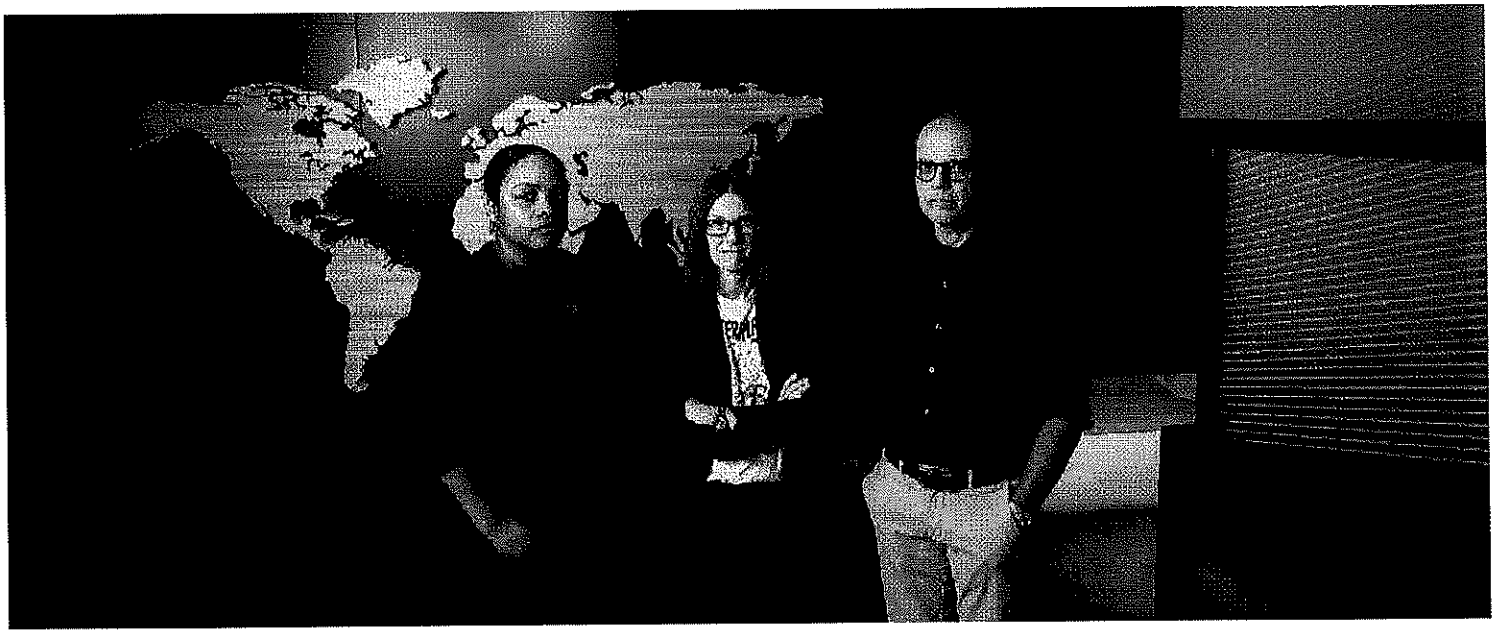
IN MY OPINION ARIZONA WOULD BE HARDER TO USE THE FRAUD I'M SUSPECTING OCCURRED SINCE COUNTY NAMES MAY BE UNIQUE BESIDES SANTA CRUZ, WHICH DOESN'T CONTAIN PHOENIX, SO AN INVASION WOULD BE NECESSARY, AND WE SEE THAT OCCURRING VIA REPORTED CARTEL INVOLVEMENT THERE. THIS WAS ALSO PERFORMED REPORTEDLY VIA CYBER CRIMINAL ACTIVITY VIA MOBILE APPS, AND THAT CERTAINLY ALIGNS WITH PRETTY MUCH EVERYTHING ELSE WE'RE SEEING HERE.



IN MY OPINION THIS, ESPECIALLY WHEN APPROPRIATELY LINKED WITH PAST EVENTS, AND TARGETING OF CATHOLICS AND CATHOLIC HEALTH INSTITUTIONS...
IN LINE WITH REPEATED ATTEMPTS TO OUST OUR HONORABLE KENNEDYS AND HONORABLE JOHNSONS, AND HONORABLE CONNALLYS AND CONNOLLYS...

IT'S TRULY LIKE A "FLASHING RED NEON SIGN" POINTING TO BAD APPLES AND THEIR INTOLERABLE BAD BEHAVIORS. IN MY OPINION IT'S TREASON AND A COUP.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice BY HAMAS? (INQUIRY)



Work & Life

Inside the fight against hackers who disrupted hospitals and jeopardized lives

Written by
Vanessa Ho

Published
July 31, 2023

Page 9.
Reference against HAMAS using cryptocurrency, etc.

Reference against attacks on public sector and health care.

After tricking an employee with a phishing email and a poisoned spreadsheet, hackers used the employee's infected computer to break into Ireland's public health system and tunnel through the network for weeks. They prowled from hospital to hospital, browsed folders, opened private files and spread the infection to thousands of other computers and servers.

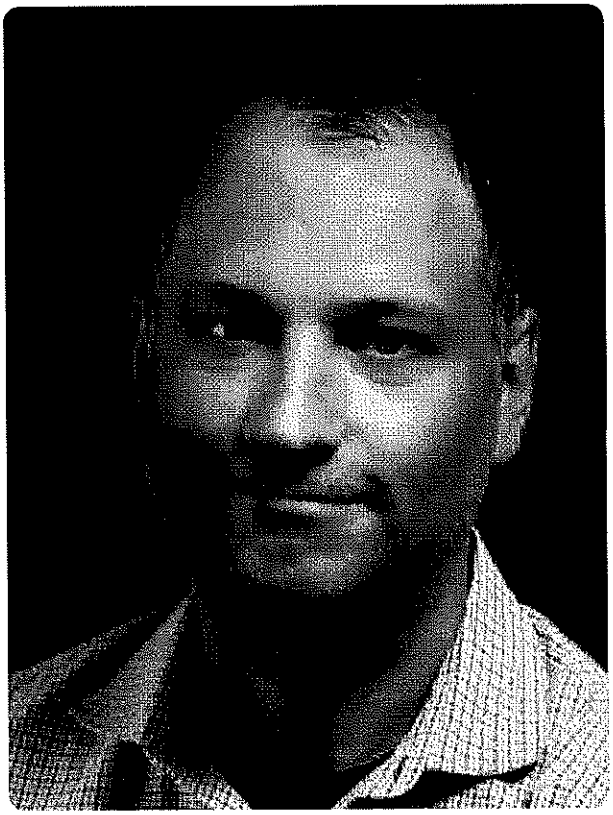
By the time they made their ransom demand, they had hijacked more than 80% of the IT system, forcing the organization of over

100,000 people offline and jeopardizing the lives of thousands of patients.

The attackers unleashed the 2021 assault on Ireland's Health Service Executive (HSE) with help from a "cracked," or abused and unauthorized, legacy version of a powerful tool. Used by legitimate security professionals to simulate cyberattacks in defense testing, the tool has also become a favorite instrument of criminals who steal and manipulate older versions to launch ransomware attacks around the world. In the last two years, hackers have used cracked copies of the tool, Cobalt Strike, to try and infect roughly 1.5 million devices.

But Microsoft and Fortra, the tool's owner, are now armed with a court order authorizing them to seize and block infrastructure linked to cracked versions of the software. The order also allows Microsoft to disrupt infrastructure associated with abuse of its software code, which criminals have used to disable antivirus systems in some of the attacks. Since the order was executed in April, the number of infected IP addresses has since plummeted.

"The message we want to send in cases like these is: 'If you think you're going to get away with weaponizing our products, you're in for a rude awakening,'" says Richard Boscovich, assistant general counsel for Microsoft's Digital Crimes Unit (DCU) and head of the unit's Malware Analysis & Disruption team.



Jason Lyons (photo courtesy of Lyons)

The effort to knock cracked Cobalt Strike offline began in 2021 when DCU — an eclectic, global group of cybercrime fighters — wanted to make a bigger dent on the rise in ransomware attacks. Previous operations had targeted individual botnets like Trickbot and Necurs separately, but ransomware investigator Jason Lyons proposed a major operation targeting many malware groups and focused on what they had in common: their use of cracked, legacy Cobalt Strike.

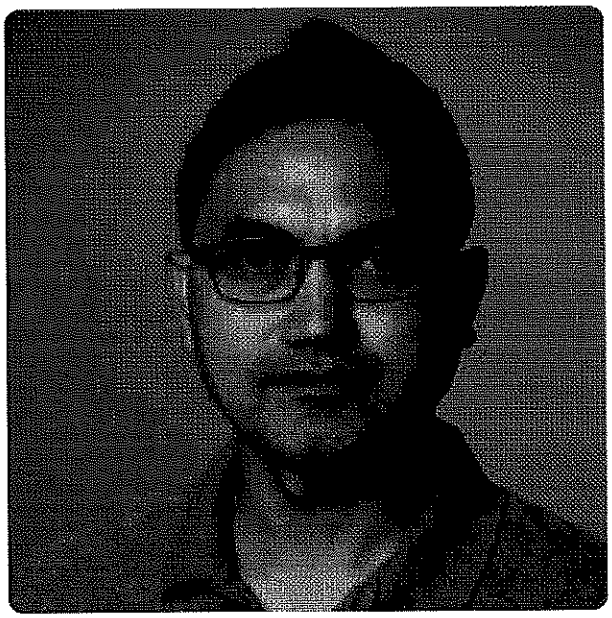
"We kept seeing cracked Cobalt Strike as the tool in the middle being leveraged in ransomware attacks," says Lyons, who based his assessments on internal intelligence of attacks on Windows customers.

A former counterintelligence special agent with the U.S. Army, Lyons had spent many nights and weekends responding to ransomware events and breaches. The chance to go after many

criminals at once was a way to "bring a little pain to the bad guys and interrupt their nights and weekends, too," he says.

But before Microsoft could start inflicting pain, it needed to clean its own house first and rid Azure of cracked Cobalt Strike. Rodel Finones, a reverse engineer who deconstructs and analyzes malware, quickly went to work. He had moved to DCU from the Microsoft Defender Antivirus team a few years ago to take a more proactive role in fighting crime.

Finones built a crawler that connected to every active, public-facing Cobalt Strike command-and-control server on Azure — and later, the internet. The servers communicate with infected devices and allow operators to spy on a network, move laterally and encrypt files. He also began investigating how ransomware operators were abusing Microsoft's software in their attacks.



Rodel Finones (photo courtesy of Finones)

But crawling wasn't enough. Investigators faced a challenge in how to distinguish between valid security uses of Cobalt Strike and illicit uses by threat actors. Fortra issues a unique license number, or watermark, for every Cobalt Strike kit it sells, which provides a forensic clue in cracked copies. But the company wasn't part of the

initial operation, and DCU investigators worked alone to build an internal catalog of watermarks linked to customer attacks as they cleaned up Azure.

Meanwhile, Fortra, which had acquired Cobalt Strike in 2020, was also working on the problem of criminals using cracked copies. When Microsoft proposed a joint operation, the company needed time to make sure partnering with Microsoft was the right move, says Bob Erdman, associate vice president for Research & Development at Fortra.

At one point, Microsoft tried to buy a copy of Cobalt Strike to help investigators understand the tool. Fortra said no.

"It's an interesting and funny story now, but we didn't know if Fortra was going to partner with us," says Lyons.

"We don't just sell to anybody who wants it," Erdman said in response.

Fortra joined the action in early 2023 and provided a list of more than 200 "illegitimate" watermarks linked to 3,500 unauthorized Cobalt Strike servers. The company had been doing its own investigations and adding new security controls, but partnering with Microsoft provided access to scale, additional expertise and another way to protect its tool and the internet. Over the course of the investigation, Fortra and Microsoft analyzed approximately 50,000 unique copies of cracked Cobalt Strike.

"It really was a very good match for the two of us," says Erdman. "It's a great way to partner where everybody's stronger working together."

The partnership was also a win for Microsoft, with Fortra's insight and watermark list greatly expanding the operation's reach. It helped the companies with their lawsuit linking malicious

infrastructure to 16 unnamed defendants, each one a distinct threat group.

Mia Scavella-Little (left), Amy Hogan-Burney (center) and Richard Boscovich in the situation room at the Microsoft Cybercrime Center, which houses DCU, in Redmond, Washington (photo by Dan DeLong)

Lawyers argued that the groups — ransomware developers, extortionists, victim lurers, cracked Cobalt Strike sellers — worked together in a bustling, lucrative ransomware-as-a-service enterprise designed to maximize profit and harm. They also linked cracked Cobalt Strike to eight ransomware families, ranging from LockBit, a fast encryption and denial-of-service attacker, to Conti, the malware suspected in the devastating 2022 attacks on the Costa Rican government.

Conti was also suspected in the Ireland attack, whose details come from a post-incident report commissioned by Ireland HSE. HSE's transparency and willingness to share what it learned is helping other organizations strengthen their defenses against cyberattacks.

Many victims attacked with cracked Cobalt Strike have been health care organizations forced to cancel surgeries, divert ambulances and delay treatment. That trend prompted Health-ISAC, a cyberthreat information-sharing association of 800 health organizations, to join the lawsuit as a co-plaintiff.

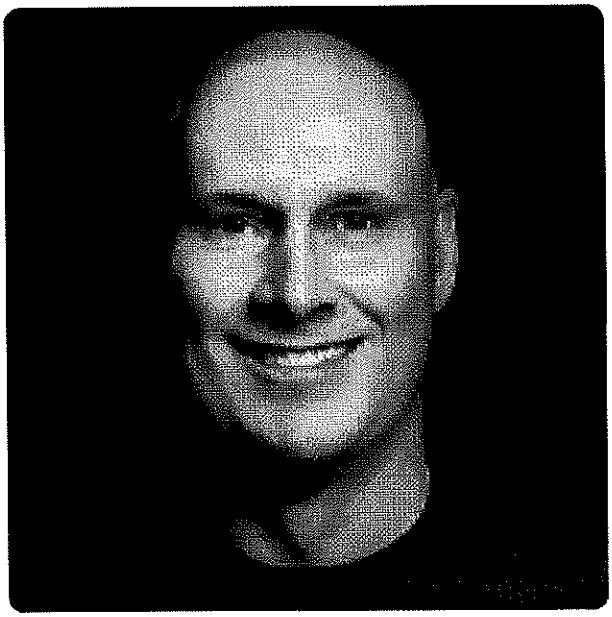
"We're talking about people's lives being at stake," says Errol Weiss, Health-ISAC chief security officer.

As the team prepared its legal arguments, DCU attorney Mia Scavella-Little helped investigators write their declarations, using her background as a data scientist to meld technical and legal language. Or, as she puts, it: "Putting 'geek' into something that actually makes sense to attorneys or a judge."

A former counterterrorism analyst for the U.S. government and a pro bono advocate, she enjoyed the purpose-driven nature of the operation.

"My career, it's mission-focused, so I like to go in there and protect and save, and that's what DCU is doing," she says.

Lawyers argued that Fortra and Microsoft have the right to take down cracked Cobalt Strike infrastructure because the threat groups broke copyright laws and terms of service. When a federal judge agreed and signed an emergency order, malware investigator Christopher Coy was ready to go.



Chris Coy (photo courtesy of Coy)

He had spent much of his time building an automated system to notify data centers and hosting providers to take down targeted IP addresses. He worked with registries to seize domains. He carefully checked through criteria for making sure Microsoft was disrupting threat actors and not innocent victims.

"One of our main concerns with all of our operations is we want to take down malicious infrastructure," Coy says. "We don't want to take down somebody's legitimate infrastructure or business that has been compromised by the bad actor. So we go through a pretty rigorous process."

The impact has been swift and promising, with all malicious .com and .net domains seized within 24 hours of the judge's order. Microsoft seized and "sinkholed" a total of 153 U.S. domains with victim traffic now going to the company's computers and away from criminal operators. And it sent notices to third parties to take down more than 1,900 global IP addresses.

The number of cracked Cobalt Strike servers detected per day — nearly a thousand when the operation began — has declined by 25% globally and 50% in the U.S. The number of victim IP

addresses infected by malicious servers on seized domains has dropped by roughly two-thirds, according to data from Microsoft's Cyber Threat Intelligence Program. The work has led to criminal referrals, recovery help for victims, continued monitoring and more legal action.

Already, threat actors are adapting, moving away from the U.S., where third parties are quick to respond to copyright infringement notices, and relocating servers in China and Russia. [and maybe Iran.]

"We know this is going to be an ongoing fight, as criminals are always shifting their tactics," says Amy Hogan-Burney, who leads DCU. "But we're persistent and committed to doing this as long as it takes."

The goal is for attacks to drop as criminals find it harder to make money with less access to efficient tools like Cobalt Strike and Microsoft APIs.

"Cybercriminals are, in a very rudimentary perspective, businesspeople too," Boscovich says. "They're saying, 'It's not worth setting anything up here because within two to three days, it's taken down.'"

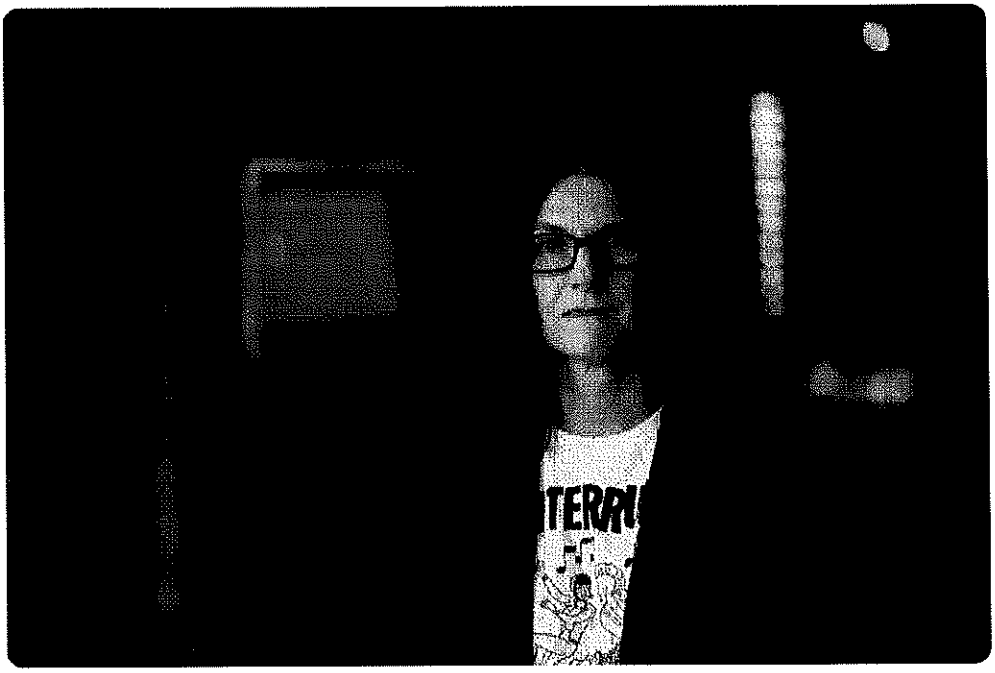
A former federal prosecutor, Boscovich joined DCU when it started in 2008 and soon developed what would become Microsoft's overall legal strategy for fighting malware. He's led 27 malware operations in the last 15 years and is continually refining the company's strategies. This year for the first time, he leveraged a racketeering law against multiple criminal groups to maximize impact.

> "The message we want to send in cases like these is: 'If you think you're going to get away with weaponizing our products, you're in for a rude awakening."

For Hogan-Burney, the results are validation of the team's experience and partnerships. Microsoft is one of few companies with a broad array of experts — attorneys, investigators, engineers, analysts — solely dedicated to cybercrime disruption. Many have military or government backgrounds and perspectives outside the company that help them work with partners, an essential part of the job, she says. And many come from careers built on protecting people, a mission they carry today.

"Every single person inside DCU is incredibly mission-oriented," says Hogan-Burney, a former FBI attorney and the general manager and associate general counsel for Microsoft Cybersecurity Policy & Protection, which oversees DCU.

"They pride themselves on doing everything they can to protect Microsoft customers and the broader internet ecosystem, and that mission-oriented drive they had beforehand, they bring it here."



Amy Hogan-Burney (photo by Dan DeLong)

That's certainly true for Coy, a Microsoft engineer for more than 25 years and a longtime U.S. Navy Reserve commander and intelligence officer. Throughout his career, he's built and shipped many products that helped people, but his role at DCU allowed him to have a bigger impact. Cracked Cobalt Strike was the last project he worked on before retiring this month.

"The work we do at DCU is having a significant impact on the security and safety of the internet as a whole," Coy says. "We're not just cleaning it up for Azure. We're trying to clean it up for the planet, and that's super rewarding and fulfilling when you're able to do that as your day job."

Top photo: Mia Scavella-Little (left), Amy Hogan-Burney (center) and Richard Boscovich at the Microsoft Cybercrime Center, which houses DCU, in Redmond, Washington (photo by Dan DeLong)

Tags:

Customers | Security

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Surface Studio 2+

Copilot in Windows

Microsoft 365

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft Industry

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States) Your Privacy Choices

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads

jt4590@protonmail.com

From: ThorfinThunder | GoldGrenade <jt4590@protonmail.com>
Sent: Saturday, September 2, 2023 11:31 PM
Subject: Fw: Opinion

The major "Heartbleed Bug" and other ransomware attacks occurred against Ascension Health during this time that I'm describing events referenced here. Henry County was unfortunately hacked and experienced ransomware due to the attacks.

------- Forwarded Message -------
From: ThorfinThunder | GoldGrenade <jt4590@protonmail.com>
Date: On Saturday, September 2nd, 2023 at 11:25 PM
Subject: Opinion
To:

https://en.wikipedia.org/wiki/Ascension_(healthcare_system)

Project Nightingale [edit]

The *Wall Street Journal* reported on a collaboration between Ascension and Google in 2019 to sha technology company. Known as Project Nightingale, the stated purpose of the collaboration was to patient records.[26] The partnership drew criticism over privacy concerns and the potential for violat Accountability Act, and the U.S. Department of Health and Human Services opened an investigatio professor of public health at Texas A&M University, noted that the Nightingale Project could improv minorities that are underrepresented in clinical studies, but also raised the lack of a patient opt-out accountability processes as concerns.[29]

Project Nightingale wasn't the first project where this occurred, but I haven't added to Wikipedia:
Merge Cardiovascular's Reporting System and IBM Watson were the first attempt, and sudden and extreme layoffs of both Ascension Health and IBM may have occurred some time afterwards.

The project also happened after one of the last Sisters, the Nuns, were no longer with Ascension.
It appears this was attempted again with project Nightingale and the Google AI system according to Wikipedia, but with the same extreme concern that employees expressed during the first attempts to connect a non-functioning reporting system and IBM's Watson.

I did my job and ensured the reporting system could work, without credit, but I still had the documentation in the cloud, which may be part of the reason why I no longer have a job.

If I have no restitution, no reparations, and similar firings while falsely identified as a threat by bad apples and their intolerable bad behaviors, at some point, the information would no longer exist, just as I had to scuttle all patient data backups meant for disaster recovery.

In my opinion, I have the misfortune of actually being someone who has worked on extremely hard projects where... nationally they had no one else who was, at that

time, simultaneously employed by Ascension Information Services/Ascension Health/St. Vincent, with the specific skillset and niche that I had been performing for years since FujiFilm Medical Systems, USA. I was the youngest person FujiFilm hired officially and the first person they hired into the position I was in without already having a Bachelor's degree.

When I say this, I say it without personal braggadocio, and simply state it factually.

Ascension Health/St. Vincent had no other employee with the skillset that I possessed to not only repair the FujiFilm Medical System (Synapse Cardiovascular) database, but also to enable the IBM Watson Health (Merge Cardiovascular) systems to integrate with it due to each system's design and database standards.

They also had no other employee who was simultaneously a Domain Admin, able to decipher how the Merge Cardiovascular Reporting System interfaced with Microsoft's Active Directory, nor another who determined how each of the separate Merge Cardiovascular software programs could be installed in a seamless way allowing SCCM to implement them. The management at Ascension Health asked nationally two times to attempt to find a team who could perform the tasks I was required to complete but failed.

This doesn't mean other employees who specialized in each of these niches didn't help me, but I was creating the design, correcting the databases, training the project managers... ensuring that we followed protocols, with assistance from other qualified professionals.

I was performing the role of a Chief Information Officer and a leader in that organization, all the way to the executive review board, while performing the tasks of potentially four people.

My regular workday was 16 hours long and went until 4am sometimes to ensure the project that they assigned me, which was 6 months behind when they hired me, succeeded.

I was rewarded with being identified as a threat, and wrongfully terminated, along with other members of the team who were aware of the gross mismanagement occurring.

The intolerable bad behavior of the bad apples who did this and ruined careers not only affected the workers, but it also may have been why the Cardiovascular software crashed, causing patient delays and a shutdown of the Indianapolis St. Vincent Cardiology systems.

I was never promoted, despite having the highest performance review and raise of any employee on my entire floor, but was instead later wrongfully convicted in an event outside of the hospital due to the interference of another bad apple I've mentioned. I was never given the job title of the positions I was required to perform, but also retaliated against for attending family funerals and laid off, despite performing all job functions and more above all expectations. They wouldn't even discuss severance with me and it's happened again.

May this be a complete and utter annihilation of all my rights, along with mine and my wife's entire livelihood, careers, and a complete besmirchment of someone who saved lives?

There is no way we can ever recover...
But when that honest truth is said, bad apples pretend I'm suicidal or homicidal when

I'm neither, and pretend I'm a threat to society, and to my knowledge are never prosecuted.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice

jt4590@protonmail.com

From: ThorfinThunder | GoldGrenade <jt4590@protonmail.com>
Sent: Sunday, August 20, 2023 1:23 AM
To: whistleblower@ronjohnson.senate.gov
Subject: Re: Dear Esteemed FBI Director Wray

You might consider a FOIA request rather than a subpoena at first since I'm applying for a career with our esteemed FBI, and they've been kind and helpful along this process.

In my opinion, they may be forthcoming, or they may have provided information already regarding the Thorfinnr files and laptop when you met with our Esteemed Christopher Wray.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice
-------- Original Message --------
On Aug 19, 2023, 2:49 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:

> -------- Original Message --------
> On Aug 1, 2023, 5:46 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:
> Attached.
>
> **Sincerely,**
> **Jon F. D. Turpin, Pro Se, Pro Hac Vice**
> **Commander-in-Chief Custodial Consulting**
> FBI InfraGard Louisiana & Indiana Chapters
> Fritz Technology LLC & Turpin Electric, Inc.
>
> E-mail: jt4590@gmail.com
> E-mail: jt4590@protonmail.com
> Phone: +1 225 259 6270
> Phone: +1 225 228 5466
>
> BAS in CIT - IUPUI
> AAS in CIT Networking & Security - Ivy Tech
> "A successful man is one who can lay a firm foundation with the bricks others have thrown at him." -David Brinkley
>
> Sent from Proton Mail mobile
>
> -------- Original Message --------
> On Aug 1, 2023, 3:51 AM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:
>
> Now I'm going to tell you a story, and I want you to understand that this is not me tooting my own horn, but something that must be said now because too many things may not be coincidental anymore.
>
> I performed what may have been the largest data migration of cardiovascular data for St. Vincent/Ascension Health, and the hospital that sits next to our Honorable Terry A. Doughty, St. Francis,

I also may have repaired their cardiovascular database in the past.

I'm also the man who fixed Yale University's cardiovascular database, along with repairing a multitude of other cardiology databases around the nation like Foothill Cardiology.

But St. Vincent/Ascension Health is very important, because of how much area these hospital systems cover, and even more important for how many patients they see and luves they save, and how overwhelmingly necessary they became during COVID.

When I entered St. Vincent the database migration was 6 months behind and I was assigned a task that I was told was impossible, and yet I succeeded, not only in the migration into a less sophisticated software solution, despite it being 10 years newer than the existing Fujifilm software, but I also corrected the current database so it aligned with the qualified physicians and nurses updates, you know, the professionals regularly seeing the patients...

Even my grandfather's death and a best friend's death in an accident were used against me while I was completing this project, and some of that turmoil was caused by a few potential bad apples while I was making sure everyone's loved ones, including mine, would have physicians with access to working software, with accurate data to review even in dire situations like when a physician had to perform open heart surgery.

I used to work directly, via phone call at least, with Dr. Feigenbaum from IU Health, the man who helped pioneer some of the lifesaving techniques improved upon and still used today, and he trusted me to keep his cardiology software and machine running so he could do his best work for all of us.

Here's my point, when I did my job properly, I was laid off for illegal write-ups, then that person tried to classify me as a threat because they got caught trying to connect networks without vetting them in a way which might have shut off machines and could potentially have caused patients not to be seen in time for preventative and/or life saving procedures.

I gave them all the tools they needed to succeed without any malice, and said it was truly concerning, so they fired my HR person, too, just to shove me out the door faster.

The software crashed later without me having any ability to access it, after I had reported any and all of my accounts on the way out of the door to ensure security... I used to be a domain administrator with full access and even ensured that was locked.

When it crashed I offered to fix it for free, and I went back and helped without any malice.

Who identifies a man willing to fix software keeping people alive for free as a threat?

I didn't even sue, and I was actively applying for the CIO position, but unfortunately the bad apple may have been applying for it, too.

May this be motive to falsely identify me as a threat and proclaim that I was suing?

May I have been trying to protect patients?

May this situation be similar?

If I've been "fired" maybe I did my job right?

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice
Commander-in-Chief Custodial Consulting
FBI InfraGard Louisiana & Indiana Chapters
Fritz Technology LLC & Turpin Electric, Inc.

E-mail: jt4590@gmail.com
E-mail: jt4590@protonmail.com
Phone: +1 225 259 6270
Phone: +1 225 228 5466

BAS in CIT - IUPUI
AAS in CIT Networking & Security - Ivy Tech
"A successful man is one who can lay a firm foundation with the bricks others have thrown at him." -David Brinkley

Sent from Proton Mail mobile

-------- Original Message --------
On Aug 1, 2023, 3:21 AM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:

If the question here about whether or not to give back FISA access to our Esteemed FBI is in regards to database searches that happened, then I have an opinion.

I already forgive our Esteemed FBI for reviewing me, and in my opinion our Esteemed Christopher Wray and our Esteemed FBI under his direction are helping to keep us safe and clean up a mess like dedicated public servants and they're earning their keep, and our Esteemed James B. Comey was trying his heart out, too.

It's part of our Faith to forgive and we do.
That being said, I have another opinion.

As a database expert and consummate professional who has worked on a multitude of our Healthcare IT systems and other valuable systems with the utmost care:

In my opinion the reason that our Esteemed Christopher Wray is letting our Honorable Mike Johnson know that the searches were unintentional, may be because they were potentially caused by Malware or external origin that was purportedly found in our government systems recently.

The amount of searches that happened in such a short span of time just doesn't sound like a human operation nor assigned task to me, that sounds like an attack, very similar to the attacks which I believe I experienced via foreign agents and what may have infected one of my phones, and potentially our Honorable Hillary D. R. Clinton's phones in the past which were purportedly smashed.

We know that Seal Team 6 has technology access to functions within cell phone chips that allow them to help our country and ensure our safety, and we know that ever since Apple and Qualcomm may have been attacked and since we found malware in potentially even our judiciary systems that there is an issue only the experts may solve.

I'm merely using the technology of Seal Team 6 as an example here, our military and veterans heroes who sacrifice for us every day, not equating them with bad apples.

I'm not a hacker but I've encountered malware, I mostly fix things and do puzzles, that's pretty much my "thing" but I do notice when things are "off" and not functioning, and may sometimes be able to identify what the potential causes may be, and in my opinion, that sounds like a malware attack.

In my opinion, too many queries in too little time for just FBI agents causing an issue, and no reason to hurt Esteemed FBI messengers nor our Esteemed Christopher Wray.

It sounded like something automated to me, and when I reported, it seemed that turned out to be the case, so in my opinion, which is potentially qualified here, not a stretch, and truly not our, nor our Esteemed FBI's fault.

Sincerely,

Jon F. D. Turpin, Pro Se, Pro Hac Vice
Commander-In-Chief Custodial Consulting
FBI InfraGard Louisiana & Indiana Chapters
Fritz Technology LLC & Turpin Electric, Inc.

E-mail: jt4590@gmail.com
E-mail: jt4590@protonmail.com
Phone: +1 225 259 6270
Phone: +1 225 228 5466

BAS in CIT - IUPUI
AAS in CIT Networking & Security - Ivy Tech
"A successful man is one who can lay a firm foundation with the bricks others have thrown at him." -David Brinkley

Sent from Proton Mail mobile

-------- Original Message --------
On Aug 1, 2023, 1:59 AM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:

To me what is concerning without laying blame on present company nor our Esteemed Governmental agencies, is that this situation may have been so targeted by specific bad apples and their bad behaviors, that I was actually double taxed, and paid it without blaming our Esteemed IRS, because I forgive them already and anyway, but may have been made into a dual citizen of each state, and for a time I was in fact in each InfraGard.

What I'm saying is: I didn't cause that, and I didn't even realize it was possible until it happened with me just working from home, taking care of my wife and cats, even when I had broken bones in my back from the nightmare we endured, yet potentially the same bad apples sent unnecessary welfare checks to our door when we were keeping to ourselves except to say hi to a few people, being kind to our neighbors, going to church, feeding our cats, and mowing our lawn.

What I'm trying to say is, in my opinion this may mean I had every responsibility to report out of concern properly to the appropriate personnel in each state, and the right, and/or potentially responsibility to speak to our Honorable Public Officials in each state, as a rightful member of our FBI InfraGard in each

state, and a whistleblower filing not for money, but instead simultaneously in support of each of our states, and in support of our Esteemed Governmental agencies, and in support of our Honorable Robert F. Kennedy, and our Honorable Eric Holcomb, and each state's Honorable Attorney Generals, but also without playing favorites because aren't you all public servants and doing your best?

When I say that our Honorable Robert F. Kennedy, Jr. deserves protections, I also think that our other Public Officials, even if someone's Honorable status might be questioned, as unfortunately happens from time to time, deserve protections and shouldn't be harmed, but in my opinion it doesn't mean we can't report out of concern.

I forgive Mike Johnson's staff already, if they even were concerned at all, so far they didn't tell me, and if they did I would just sincerely apologize, but I also know I followed the directions on the door... and I'm not trying to cause them issues, at all. In my opinion he and his staff along with many of our other representatives are doing so much for all of us, I just don't want to be forgotten when I, like so many of us, didn't even make the mess we're experiencing and thrown into.

There's an old saying about not hurting the messenger, and I'm paraphrasing, because in my opinion, it can be said more tamely.

Don't hurt the messenger... why not instead take the work I put together and let everybody else look good, but not allow us to be destroyed in the process?

Why not consolidate my information under our Honorable Kennedys and allow our Honorable Jeffrey Landry and Honorable Todd Rokita, and Honorable Kennedys and Honorable Johnsons to use that money for our great state of Louisiana, just like I asked for the business that was stolen from me to be used for our Great State of Indiana, and the car that was tampered eith to be used for our Respected Indiana State Police?

Just like I asked for any illicit cryptocurrency that bad apples may have attempted to throw off on me to be used for our Esteemed IRS, Esteemed FBI, and rewards for the international criminals I may have caught to be used for our Great State of Georgia and maybe any other state that may have some potentially valid complaints, not about us, but that we don't want to talk about nor even to know are complaints if no one hurts the messenger.

Was it too much to ask to simply be restored in all of that if I'm asking everyone to get along and not allow me to be slapped around by bad apples for them to simultaneously try to force me to have an opinion, then try to slap me around some more because my opinion may be one that stops the turmoil?

In whatever way and however each of our Honorable Representatives and Esteemed Agencies sort it out could it please not include allowing potential bad apples to take our rights away again in some dystopian perpetually repeated double jeopardy?

What I'm trying to say is, I wasn't ever trying to fight anyone, I was trying to be away from this turmoil and let everyone else handle it after I made my required reports out of concern, but some bad apples kept forcing me to be necessary and important against my will, but simultaneously trying to act like I was a threat for ensuring no one got harmed.

Who does that?

Who made such a mess that it dragged in a Catholic autistic guy who donates to Children's Hospitals even at a loss?

Who made such a mess that it dragged in a guy who has been forgiving everyone?

Who keeps trying to act like I'm some kind of threat for following oaths and guidelines?

Who made such a mess that I may have the right, which I'm not using and not trying to push the issue on, but just... factually may have the right... to vote in two states?

Who is acting like me knocking on a door and ringing a doorbell once is concerning?

I didn't even complain about our respected law enforcement when a potential bad apple wasted their valuable time sending them to our door for unnecessary welfare checks...

Who is acting like me following directions to slip something under a door for security, and speaking to a building manager to ensure a securely encrypted package is delivered and in a monitored, secure area is concerning?

Are they ok?

Sincere question, but in your purview because I'm not trying to find out for myself nor even bother anyone by breathing wrong, I'm trying to peacefully stay alive with all my rights because bad apples being allowed to hurt me also hurts my wife, and I think family people understand that's just the facts.

Why didn't someone just ask me for whatever it was that they wanted and stop the threats?

Why did someone surveille me and potentially have me followed with P.I.s when I was already going to apply for our Esteemed FBI, had already asked for Witness Protection, and would have willingly signed a standard form 50 and just kindly cooperated?

What is the issue?

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice
Commander-In-Chief Custodial Consulting
FBI InfraGard Louisiana & Indiana Chapters
Fritz Technology LLC & Turpin Electric, Inc.

E-mail: jt4590@gmail.com
E-mail: jt4590@protonmail.com
Phone: +1 225 259 6270
Phone: +1 225 228 5466

BAS in CIT - IUPUI
AAS in CIT Networking & Security - Ivy Tech
"A successful man is one who can lay a firm foundation with the bricks others have thrown at him." - David Brinkley

Sent from Proton Mail mobile

-------- Original Message --------
On Jul 31, 2023, 9:12 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:

In my opinion, there may be an attempt by bad apples and their bad behaviors to scapegoat me yet again by trying to make me seem like a threat for peacefully doing what is required by our constitution, jurisprudence, the FBI InfraGard PIN, and as a Whistleblower who has already successfully served any time in advance by jurisprudence as well.

In my opinion, this may be what bothers these bad apples with their bad behaviors, that and their odd need for control of us.

In my opinion, these may have been the same tactics attempted against Lee H. Oswald, and regardless of who thinks who did what, the loss of John F. Kennedy was a tragedy the likes of which should never occur again.

So I've requested that Robert F. Kennedy, Jr. receive a protective detail to ensure his safety when he speaks for all of us in August, and since it seems to me there are still attempts to frame me when I don't even like hurting an ant, much less pets, and especially don't like hurting human beings...

I'm here to tell you I like Robert F. Kennedy, Jr.'s voice, because in my opinion he speaks honestly and all our Honorable Kennedys like the rest of us and God's Creatures, deserve to be heard and have our constitutional rights.

So give that man the protection he deserves, because as a plain clothes citizen I was still willing to stand in front of him and make sure he was safe, but since there's such an insane effort to pretend I'm a problem for being safe, responsible, prudent, and potentially correct:

Protect our Honorable Robert F. Kennedy, Jr.
That is my opinion, out of genuine concern.

Whomever keeps trying to have this both ways on us, just tell them no, and mean it.

With all due respect, please, and thank you, this really needs to stop before any bad apples try to "bury us with money" at the turn of the fiscal year just to control a narrative.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice
Commander-In-Chief Custodial Consulting
FBI InfraGard Louisiana & Indiana Chapters
Fritz Technology LLC & Turpin Electric, Inc.

E-mail: jt4590@gmail.com
E-mail: jt4590@protonmail.com
Phone: +1 225 259 6270
Phone: +1 225 228 5466

BAS in CIT - IUPUI
AAS in CIT Networking & Security - Ivy Tech
"A successful man is one who can lay a firm foundation with the bricks others have thrown at him." - David Brinkley

Sent from Proton Mail mobile

-------- Original Message --------
On Jul 31, 2023, 6:11 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:

I met Lynn in Shreveport, LA today after the OSC identified me as a whistleblower in an email. I'm not sure why her demeanor was to act like I was an issue for knocking once on our Honorable Mike Johnson's door.

I was asking him to support you and your FISA access, just like I wanted to sincerely ask our Honorable Joshua Hawley.

Lynn informed me I was removed from the FBI Infragard for being unemployed even though I have my own business, and despite my job being lost due to other falsely identifying me as a threat when I haven't hurt anyone and have put years into keeping my oaths and trying to follow every rule of our FBI Infragard.

Why is Lynn doing that?
Is Lynn trying to discredit me even though I support our esteemed FBI?

In my opinion my reports were quite cohesive, and took a lot of time and money and even blood, sweat, and tears, to submit.

I have no issue with Lynn, but if so, when does this stop?

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice
Commander-In-Chief Custodial Consulting
FBI InfraGard Louisiana & Indiana Chapters
Fritz Technology LLC & Turpin Electric, Inc.

E-mail: jt4590@gmail.com
E-mail: jt4590@protonmail.com
Phone: +1 225 259 6270
Phone: +1 225 228 5466

BAS in CIT - IUPUI
AAS in CIT Networking & Security - Ivy Tech
"A successful man is one who can lay a firm foundation with the bricks others have thrown at him." -David Brinkley

Sent from Proton Mail mobile

jt4590@protonmail.com

From: ThorfinThunder | GoldGrenade <jt4590@protonmail.com>
Sent: Saturday, August 26, 2023 4:51 PM
To: pinkerton.info
Subject: Re: Dear Honorable Pinkertons

Here's another list of potential issues:
Borg Warner (Transmission Heat Treat Process)
Daimler Chrysler (8-Speed Transmissions & Pentastar Engines Oil Pressure)
[May simply be an error in the heat treat process manufacturing due to complexity.]
[Please repeat QA tests on temperature and time in heat treat after T-5/T-56 models.]
[Someone I knew designed some processes and... math is not their strength so I can easily see potential for honest mistakes in such difficult process designs and implementation.]

The recall reported in the 2017 Jeep Compass still occurs in the Jeep Compass 2020, but it's the oil pressure and coolant lights that come on before the car loses power, and it does this even when it has the proper amount of oil, and the proper amount of coolant in them:
https://tflcar.com/2022/12/jeep-compass-safety-issue-loss-of-motive-power-investigation/

The issue with the transmissions and the oil pressure would align with the hairline fractures found in VW Beetle and other related engines dealing with the loss of oil pressure as well.

In my opinion, each of these issues would only be able to occur readily if one process underlying each issue has an honest mistake occurring, and that would be heat treat.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice

------- Original Message -------
On Friday, August 25th, 2023 at 5:02 PM, ThorfinThunder | GoldGrenade <jt4590@protonmail.com> wrote:

> Potentially Sabotaged:
> IBM (Underlying AI Infrastructure)
> Merative Health (Reporting Feature and Active Directory Queries)
> Dominion Voting (Database & Paper Ballots)
> Daimler Chrysler (Drivetrains and Manufacturing)
> Hagerty Insurance (Clerical Errors)
> Indiana Michigan Power (Database and Controls)
> Ninestar Connect (Internet Power and Propane)
>
> Please investigate if possible and approved.
>
> Sincerely,
> Jon F. D. Turpin, Pro Se, Pro Hac Vice
> -------- Original Message --------
> On Aug 25, 2023, 4:46 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:
>
> > Do you remember my genuine concern regarding an attack from the electric grid?
> >
> > The Ninestar Power Database links to Michigan of my memory serves me correctly.

I'm seeing a pattern occurring here and I think it's time to mobilize our Honorable Pinkertons to see what is going on here.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice

Mediaite + Follow

Chris Wray Warns Hamas Attack 'Will Serve as an Inspiration' For Terror Threats Against the U.S.

Story by Ken Meyer • 4d

He is also notifying publicly that we should be cognisant of potential attacks on the electrical grid, and/or water sources.

FBI Director **Christopher Wray** warned of the possibility that "violent extremists" will draw inspiration from Hamas' attack on Israel to make threats against the U.S. and other countries.

In a hearing before the Senate Homeland Security Committee on Tuesday, Wray said the war between Israel and Hamas "has raised the threat of an attack against Americans in the United States." He based this on threats that al Qaeda, ISIS, and Hezbollah have called for against Jews, Americans, and their Western allies.

"We assess that the actions of Hamas and its allies will serve as an inspiration, the likes of which we haven't seen since ISIS launched its so-called caliphate several

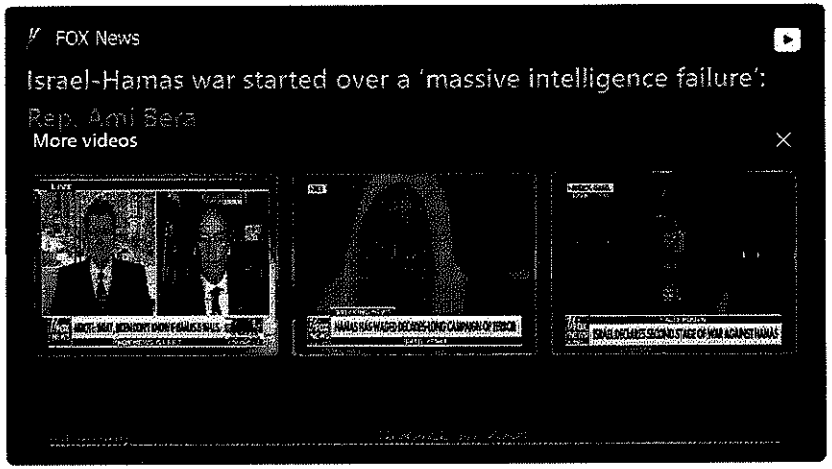
Wray assessed that America's most immediate concern is that "violent extremists — individuals or small groups — will draw inspiration from the events in the Middle East to carry out attacks against Americans going about their daily lives." As he warned about recent anti-Semitic and anti-Muslim violence in America, Wray pivoted from homegrown violence to say "We cannot and do not discount the possibility that Hamas or another foreign terrorist organization may exploit the current conflict to conduct attacks here on our own soil."

"It is a time to be concerned," said Wray. While he told Congress the FBI has "no information to indicate that Hamas has the intent or capability to conduct operations inside the U.S.," he continued to emphasize vigilance in light of the possibility.

Watch above via CSPAN.

The post Chris Wray Warns Hamas Attack 'Will Serve as an Inspiration' For Terror Threats Against the U.S. first appeared on Mediaite.

Related video: Israel-Hamas war started over a 'massive intelligence failure': Rep. Ami Bera (FOX News)



More for You

Amazon Hates When Prime Members Do This, But They Can't Stop You

Online Shopping Tools

Amazon Hates When Prime Members Do This, But They Can't Stop You

Ad

essanews.com

Hezbollah leader threatens the USA: "We are well-prepared"

8 20

FOX News

Democrat Rep. Ritchie Torres 'mistakenly' voted against resolution condemning...

44

Daily Post Nigeria

'Your days are numbered' – Defence Headquarters warns terrorists

390 30

The Wall Street Journal

Hamas Has Deadlier Weapons Than the Last Israel Invaded Gaza

24

Business Insider

ABC News

Business Insider

Indiana: Say Bye To Your Prime Membership If You Live In These Zips

Online Shopping Tools

American Shoppers Should Th Before Buying From These 2 Sto

Online Shoppin

Feedback

Opinion

1 message

Jon F. Turpin <jt4590@gmail.com> Sat, Nov 4, 2023 at 10:20 PM
To: "SA Joseph L. Chaney" <jlchaney@fbi.gov>, cawray@fbi.gov

I reviewed some of the documentation from the CISA regarding Dominion Voting Systems and how they're designed, and I also reviewed how they used to be designed as far back as 2008.
So far at a rudimentary glance, what I noticed is that in each instance there is the possibility of an AES key to be compromised in each of these, and that each could be targeted by known malware.

The older versions would have been extremely likely to be hit by the Cobalt Strike attack methods, which have been going on for some time, and even delete evidence of themselves after activation.
In fact, the older versions utilized Assembly Code and versions of Windows and processors now known to have allowed, unfortunately, system access via x86 coding faults, but that's less likely here.

What I see is that WinEDS 4.0, and any version running on Windows XP, Windows XP SP2, Windows Server 2003, or Windows Server 2008, and maybe R2, would have similar vectors for attacks.
That's what I identified as the most likely potential for attack besides paper ballots themselves, because the EDS server would be what counts and generates the tallies for the election in each jurisdiction.

Because there have been questions about the last 3 elections, and I'm not pointing fingers at any candidate, what I'm doing is researching these systems from the time they were anti-trusted and bought.
In my opinion, the root cause of any potential issue will be found in these older files, which is once again not to point fingers at Sequoia Voting Systems, Election Voting Systems, nor Dominion Voting.

Because the newer systems are based upon the design of the older systems, even though some of these have switched to Android, very similar potential exploits seem to exist in the newer systems as well.
When I reviewed documentation as recent as 2021 from California, I found that Windows System Builds are still mentioned in regards to the Democracy Suite EMS, which seems to be the server component.
https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510a/provv-source.pdf

1.4 System Overview

The Democracy Suite 5.10-A Voting System is a paper-based optical scan voting system consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC) ballot scanner, the ImageCast Precinct 2 (ICP2) precinct count tabulator, ImageCast Evolution (ICE) precinct count tabulator, ImageCast Voter Activation (ICVA), Mobile Ballot Printing (MBP), and ImageCast X (ICX) BMD ballot marking device.

1.5 Description of Component Code

The table below provides the component lines of code for D-Suite 5.10-A.

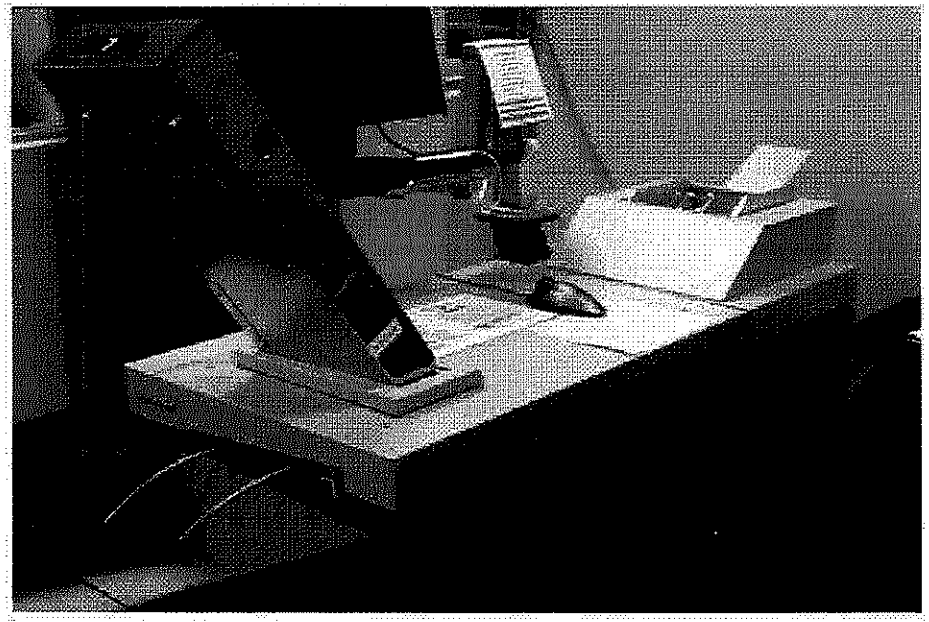
Table 1-1 Democracy Suite 5.10-A Component Lines of Code

Component	Language/s	Lines of Code	Standard
EMS*	C#	1,721,537	SD_CSharp_AutomatedCodeReview_5.10_A.pdf
ICP2	C/C++	486,907	SD_CplusPlus_CodingStandard_5.10_A.pdf
ICX	Java	224,307	SD_DVSJavaCodingStandards_5.10_A.pdf
ICE	C/C++	852,980	SD_CplusPlus_CodingStandard_5.10_A.pdf
ICC	C/C++	231,903	SD_CplusPlus_CodingStandard_5.10_A.pdf
ADJ	C#	200,913	SD_Csharp_AutomatedCodeReview_5.10_A.pdf

**Note: EMS Includes ICVA and MBP.*

Does this still utilize SQL? Many things do, which isn't a bad thing, but my reference to the susceptibility to hide changes not only to a system, but also to the transaction files within SQL via Cobalt Strike may apply.

Summary



The **Optech 400-C** is a high capacity scanner used by election officials to count ballots in a central location. The Optech 400-C originally developed by Business Records Corporation and later by both Sequoia Voting Systems and Election Systems and Software. As the result of an antitrust settlement, ES&S ceased production of the Optech 400-C in 1997 but continues to service the equipment in many jurisdictions. (In jurisdictions with maintenance contracts with ES&S the equipment is often called the Optech IV-C or Model 400.) Ballots are cast in precincts and placed in ballot boxes. The ballots are then delivered by two poll workers to the central count facility, where they are fed by an election official into the 400-C. Because it is used by election officials in a secure, central location, the 400-C does not provide voters with feedback about ballot problems.

The system consists of a high-capacity scanner linked to a PC running Microsoft Windows. The 400-C uses a proprietary tabulation program, WinETP, to process the ballots that it scans. WinEDS is used to configure the ballot definition files and precinct identifiers that instruct the 400-C's as to how to interpret each ballot voter's ballot marks. The ballot definitions are then transferred from WinEDS to the 400-C via removable media, such as USB sticks, DVDs, or floppy disks. When the 400-C is done tallying the results for the election, the results are copied from the 400-C onto a DVD or a memory cartridge and transferred to the WinEDS server. The WinEDS server combines these results with those from any Insight and Edge units used in the jurisdiction. Finally, WinEDS generates tally reports for the election.

The process is still effectively the same even if it switched to Android, and you can see this in the potential exploits listed on the CISA's Website: https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01

2.2 VULNERABILITY OVERVIEW

NOTE: Mitigations to reduce the risk of exploitation of these vulnerabilities can be found in Section 3 of this document.

2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

CVE-2022-1739 has been assigned to this vulnerability.

2.2.2 MUTABLE ATTESTATION OR MEASUREMENT REPORTING DATA CWE-1283

The tested version of ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device.

CVE-2022-1740 has been assigned to this vulnerability.

2.2.3 HIDDEN FUNCTIONALITY CWE-912

The tested version of ImageCast X has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code.

CVE-2022-1741 has been assigned to this vulnerability.

2.2.4 IMPROPER PROTECTION OF ALTERNATE PATH CWE-424

The tested version of ImageCast X allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1742 has been assigned to this vulnerability.

2.2.5 PATH TRAVERSAL: '../FILEDIR' CWE-24

The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.

CVE-2022-1743 has been assigned to this vulnerability.

2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1744 has been assigned to this vulnerability.

2.2.7 AUTHENTICATION BYPASS BY SPOOFING CWE-290

The authentication mechanism used by technicians on the tested version of ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions.

CVE-2022-1745 has been assigned to this vulnerability.

2.2.8 INCORRECT PRIVILEGE ASSIGNMENT CWE-266

The authentication mechanism used by poll workers to administer voting using the tested version of ImageCast X can expose cryptographic secrets used to protect election information. An attacker could leverage this vulnerability to gain access to sensitive information and perform privileged actions, potentially affecting other election equipment.

CVE-2022-1746 has been assigned to this vulnerability.

2.2.9 ORIGIN VALIDATION ERROR CWE-346

The authentication mechanism used by voters to activate a voting session on the tested version of ImageCast X is susceptible to forgery. An attacker could leverage this vulnerability to print an arbitrary number of ballots without authorization.

CVE-2022-1747 has been assigned to this vulnerability.

But despite the vulnerabilities listed about ImageCast X, I'm not concerned as much with the endpoint, nor even the scanner, since individuals may have been caught with extra ballots. My concern would rest with, specifically, the central component which holds the database, the EMS, which still appears to run on Windows, which is fine, but as with any OS exploitable.

How similar it is to the old systems, could anyone undetectably grab an export (It says yes, above regarding ImageCast X)
Could they change a database and/or even print a number of ballots out and potentially even make minimal changes to them? (It says yes, above regarding ImageCast X)
Since it's so similar, and the core architecture may still be very similar, could it even be taken to an older machine to have ballots printed in a way that seems legitimate?

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice

Review Page 4 (iv) in table of contents and any related documentation. In my opinion, when correlated with exhibits E1 + F1 from 2020-CV-034319, this system may have been at risk of attack via "Cobalt Strike." This proves the underlying infrastructure of the system could potentially have been able to be targeted by Cobalt Strike. Which has been found to be recently utilized by external bad apples, such as malware and ransomware groups, I'm Not blaming DAs, nor [redacted] Judges, etc. I'm Not blaming Dominion Voting. I'm Not blaming iBeta. Etc. Etc.

iBeta QUALITY ASSURANCE

Dominion Voting Systems WinEDS 4.0 VSTL Certification Test Report

Prepared for

Dominion Voting Systems

717 17th Street, Suite 310, Denver, CO 80202

EAC Application # SEQ-40-2007-WI

Version 1.0

(V)2010-08Sep-001(A)

This report has been submitted to the EAC for review and is pending their acceptance. No certification number has been issued. When iBeta receives notification that the report is accepted, a revised version of the report will be issued. The Certification number will appear here, in page headers and in Appendix K. Any other revisions will be noted in the version history.

Trace to Standards NIST Handbook 150-22	
Section 5.5, 5.10.1 through 5.10.3, 5.10.5, 5.10.6	
VSS	
Vol. #	Section(s) #
1	1.6.1
1	2, 3, 4, 5, & 6
1	9.6.3
2	2, 3, 4, 5, & 6
2	7.4 & 7.5.
2	Appendix B

Test Results in this report apply to the voting system configuration tested. Testing of voting systems that have been modified may or may not produce the same test results. This report shall not be reproduced, except in full.
iBeta Quality Assurance is accredited for Voting System Testing:

I'm Not Finger Pointing. I'm Not an "election denier."

U.S. Election Assistance Commission

VSTL

I'm submitting this out of genuine concern, showing tampering may have been possible by potential external bad apples.

EAC Lab Code: 0702 – Effective through 7/16/2011

NVLAP®

I'M JUST SEEING A POTENTIAL PATTERN.

NVLAP LAB CODE 200749-0

THIS IS 13 YEARS OLD OR MORE AND INCLUDED FOR REFERENCE TO ALLOW A REASONABLE INFERENCE OF DESIGN.

2675 S. Abilene Street, Suite 300, Aurora, Colorado, 80014

Form-E: VSTL Test Report template

Version History				
Ver #	Description of Change	Author	Approved by	Date
V1.0	Initial Release	Gail Audette Charles Cvetezar Kelly Swift Dharma Valdez Kevin Wilson	Gail Audette – iBeta Quality Manager Ed Smith – Dominion VP, Compliance and Certification Eric Coomer – Dominion Director of Product Development	8 September 2010

Trademarks

TABLE OF CONTENTS

This is the underlying source code strike may target.

1 Introduction

This report is submitted to the Election Assistance Commission (EAC) by iBeta Quality Assurance summarizing the federal voting system certification testing of the Dominion Voting Systems, Sequoia WinEDS 4.0 voting system to the *Federal Election Commission Voting System Standards 2002 (VSS 2002)*.

The Sequoia WinEDS 4.0 test campaign is an initial EAC Certification. It incorporates an Election Management System and five voting devices, two of which include two hardware models.

- The WinEDS election management system for ballot preparation and central count functions;
- The *EDGE2plus* touch screen Direct Recording Electronic (DRE) video and audio voter editable ballot devices with accessible ballot inputs for voters with manual dexterity limitations (models CO.3 and CO.4);
- The *EDGE2plus* Model 305 touch screen Direct Recording Electronic (DRE) video device;
- The Edge II touch screen DRE video voter editable ballot devices with peripheral hardware to support audio ballot and a Voter Verified Paper Audit Trail (VVPAT);
- The Optech Insight and Optech Insight Plus precinct count optical scanners; and
- The Optech 400-C central count optical scanner.

During the certification test campaign, Sequoia Voting Systems was purchased by Dominion Voting Systems. For the purposes of this final report, Sequoia WinEDS 4.0 refers to the voting system under test during this federal test campaign.

The purpose of this document is to provide an overview of the certification testing and findings. The complete list of the systems names, major subsystems, version numbers and any interfacing devices is detailed in Section 3 - Voting System Identification. Additional details of the design, structure, and processing capabilities are identified in Section 4 - Voting System Overview.

This certification test campaign included a Physical Configuration Audit (PCA) of the Sequoia WinEDS voting system which included a review of the documentation and source code submitted in the Technical Data Package (TDP) to the requirements of the *VSS 2002*.

A Functional Configuration Audit (FCA) of the Sequoia WinEDS voting system included a review of the testing performed by Dominion to:

- The requirements of *VSS 2002*;
- The WinEDS voting system specifications of the Sequoia TDP; and
- The voting system requirements of section 301 of the Help American Vote Act (HAVA).

The FCA also includes identification of the scope of testing, a test plan, customization of test cases, system configuration management, test execution, and analysis of the test results

Certification testing was performed in compliance with the requirements of *VSS 2002*, Volume 2. The test record included all test executions and reviews. All test executions and reviews included the record of requirements that were satisfactorily and unsatisfactorily completed to the accept/reject criteria identified in Appendix A, deficiencies noted, reports to Dominion, software and manufacturing resolutions, validations of resolutions and documentation of incorporation of resolutions into the voting system. During all phases of the certification testing iBeta provided Dominion with regular status reports.

iBeta Quality Assurance, a limited liability company, is located in Aurora, Colorado. The company is a full service software testing laboratory providing Quality Assurance and Software Testing for the business and interactive entertainment communities. Testing was conducted at iBeta in Aurora, Colorado.

iBeta Quality Assurance accreditations for the testing of voting systems to the federal standards include

- National Voluntary Lab Accreditation Program (NVLAP) Voting System Test Lab (VSTL)
- Election Assistance Commission Voting Systems Test Lab (VSTL)

Non-core hardware environmental testing is outside iBeta's test accreditation scope as a VSTL. This testing was performed at the following subcontractors:

- Criterion Technology, 1350 Tolland Road, P.O. Box 489, Rollinsville, CO 80474
- Oracle® Advanced Product Testing (APT), 1601 Dry Creek Drive Suite 2000, Longmont, CO 80503
- Wyle Laboratories, 7800 Highway 20 West, Huntsville, AL, 35806
- Intertek Testing Services NA, Inc., 1795 Dogwood, Suite 200, Louisville, CO 80027

Exclusions:
The following functions are excluded from the WinEDS 4.0 voting system and therefore not tested in this certification effort:

- Access to incomplete election returns or interactive queries;
- Telecommunications: No voter authentication, ballot definition, individual vote records, or voter lists are transmitted via telecommunications; and
- Shared Operating Environment: WinEDS 4.0 does not share an environment with other data processing functions.

In addition, the submitted voting system does not have components that are used external to the voting functions.

The WinEDS Voting System components supported by the WinEDS 4.0 Voting System that are not part of the certification effort include:

- Advantage D10;
- Ballot Printing System (BPS);
- WinEDS Bridge Tool;
- Eagle model optical scanners;
- Extended Services modules Teamwork and Vote Sim; and
- The EDGE2*plus* VVPAT printer which was withdrawn from the federal certification during this test campaign.

1.1 *Internal Documentation*

The documents identified below are iBeta internal documents used in certification testing.

Table 1 Internal Documents

Version #	Title	Abbreviation	Date	Author (Org.)
v1.0	Voting Certification Master Services Agreement-Statement of Work	MSA contract - SOW	30 May 2007 - 22 June 2007	iBeta Quality Assurance
	VSTL Procedures			
v3.0	Voting Deliverable Receipt Procedure		February 9, 2010	iBeta Quality Assurance
v2.0	PCA Document Review Procedure		February 4, 2009	iBeta Quality Assurance
v1.0	Witness Build Procedure		April 7, 2008	iBeta Quality Assurance
v2.0	Trusted Build Procedure		January 23, 2009	iBeta Quality Assurance
v2.0	PCA Source Code Review Procedure		April 21, 2009	iBeta Quality Assurance
v2.0	8051 Assembler Review Criteria		April 21, 2009	iBeta Quality Assurance
v3.0	80x86 Assembler Review Criteria		April 21, 2009	iBeta Quality Assurance
v4.0	C-Sharp Review Criteria		March 3, 2009	iBeta Quality Assurance
v5.0	C and C++ Review Criteria		March 2, 2009	iBeta Quality Assurance
v3.0	Java Review Criteria		April 21, 2009	iBeta Quality Assurance
v2.0	PowerScript Review Criteria		April 21, 2009	iBeta Quality Assurance
v3.0	SQL Review Criteria		April 21, 2009	iBeta Quality Assurance
v3.0	Visual Basic Review Criteria		April 21, 2009	iBeta Quality Assurance
v3.0	VB.Net Review Criteria		April 21, 2009	iBeta Quality Assurance
v2.0	Z80 Assembler Review Criteria		April 21, 2009	iBeta Quality Assurance
v5.0	Test Case Preparation		February 9, 2010	iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
	and Execution Procedure			
v4.0	VSTL Test Planning Procedure		May 23, 2008	iBeta Quality Assurance
v4.0	VSTL Certification Report Procedure		April 24, 2008	iBeta Quality Assurance
iBeta	Project Documents			
	Code and Equipment Receipt WinEDS 4.0.xxx		September 1, 2010	iBeta Quality Assurance
	PCA Document Review WinEDS 4.0.xxx		September 7, 2010	iBeta Quality Assurance
	FCA Document Review WinEDS 4.0.xxx		February 25, 2008	iBeta Quality Assurance
	EAC Clearing House Catalog for Sequoia		July 1, 2010	iBeta Quality Assurance
	Sequoia PCA Configuration		September 7, 2010	iBeta Quality Assurance
	PCA and FCA Discrepancy Report WinEDS 4.0.xxx		September 7, 2010	iBeta Quality Assurance
v3.0	WinEDS v. 4.0 VSTL Test Plan	Test Plan	April 17, 2009	iBeta Quality Assurance
	FCA Telephony and Cryptographic Test Case WinEDS 4.0.xxx		July 26, 2010	iBeta Quality Assurance
	Sequoia FCA Security Review WinEDS 4.0.xxx		September 7, 2010	iBeta Quality Assurance
	FCA Security Test - Linux Configuration Test Steps - WinEDS-4.0		August 31, 2010	iBeta Quality Assurance
	FCA Security Test - Windows Configuration Test Steps - WinEDS-4.0-IL		August 27, 2010	iBeta Quality Assurance
	FCA Security Test Case -- Network Ports Steps- WinEDS4.0-IL		August 17, 2010	iBeta Quality Assurance
	FCA Security Test Case -- Serial Ports Steps - WinEDS4.0		December 29, 2009	iBeta Quality Assurance
	FCA Accuracy Test Case - DRE		March 26, 2010	iBeta Quality Assurance
	FCA Accuracy Test Case - Optical Scan		5 November 2009	iBeta Quality Assurance
	FCA Environmental Test Case WinEDS 4.0.xxx		September 7, 2010	iBeta Quality Assurance
	FCA Characteristics Test Case WinEDS 4.0		June 17, 2010	iBeta Quality Assurance
	General 1 - CO System TC WinEDSv 4.0.xxx, v.0, v.1, v.2		v.0: December 8, 2009 v.1: June 3, 2010 v.2: August 27, 2010 v.3: September 7, 2010	iBeta Quality Assurance
	General 2 - MI System TC WinEDSv 4.0 v.0, v.1 (Regression 1)		v.0: January 7, 2010 v.1: June 14, 2010	iBeta Quality Assurance
	General 3 - IL System TC WinEDSv 4.0		8 September 2009	iBeta Quality Assurance
	General 4 - PA System TC WinEDSv 4.0.xxx		14 December 2009	iBeta Quality Assurance
	Primary 1 - WA System TC WinEDSv 4.0.xxx		5 January 2010	iBeta Quality Assurance
	Primary 2 - WI System TC WinEDSv 4.0.xxx		29 December 2009	iBeta Quality Assurance
	Primary 3 - AZ System TC WinEDSv 4.0.xxx		6 January 2010	iBeta Quality Assurance
	Primary 4 - IL System TC WinEDSv 4.0.xxx v.0, v.1, v.2		v.0: November 24, 2009 v.1: December 8,	iBeta Quality Assurance

Version #	Title	Abbreviation	Date	Author (Org.)
			2009 v.2: June 2, 2010	
	Volume 1 - Closed Primary - IL System TC WinEDSv 4.0.xxx		March 1, 2010	iBeta Quality Assurance
	Volume 1A - Closed Primary - IL System TC WinEDSv 4.0.xxx		March 1, 2010	iBeta Quality Assurance
	Volume 2 - General - WA System TC WinEDSv 4.0.xxx, v.0, v.1		v.0: March 8, 2010 v.1: March 9, 2010	iBeta Quality Assurance
	General 3R -IL System Level Regression TC WinEDSv 4.0 (Regression 1)		June 11, 2010	iBeta Quality Assurance
	General 4R - PA System Level Regression TC WinEDSv 4.0 (Regression 1)		June 17, 2010	iBeta Quality Assurance
	Primary 1R - WA System Level Regression TC WinEDSv 4.0 (Regression 1)		June 10, 2010	iBeta Quality Assurance
	Primary 2R - WI System Level Regression TC WinEDSv 4.0 (Regression 1)		May 27, 2010	iBeta Quality Assurance
	Primary 3R - AZ System Level Regression TC WinEDSv 4.0 (Regression 1)		June 3, 2010	iBeta Quality Assurance
	Volume1R System Level Regression Test Case (Closed Primary - IL) (Regression 1)		July 8, 2010	iBeta Quality Assurance
	HAAT90 R2 System Level Regression Test Case (Regression 2)		July 19, 2010	iBeta Quality Assurance
	400C Merge System Level Regression Test Case (Regression 1)		June 24, 2010	iBeta Quality Assurance
	400C Network System Level Regression Test Case (Regression 1)		June 23, 2010	iBeta Quality Assurance

1.2 *External Documentation*

The documents identified below are external resources used to in certification testing.

Table 2 External Documents

Version #	Title	Abbreviation	Date	Author (Org.)
	Test Plan Approval Letter		April 23, 2009	Election Assistance Commission
	Help America Vote Act	HAVA	October 29, 2002	107th Congress
NIST Handbook 150 2006 Edition	NVLAP Voting System Testing	NIST 150	February 2006	National Voluntary Lab Accreditation Program
NIST Handbook 150-22	NVLAP Voting System Testing	NIST 150-22	October 2007	National Voluntary Lab Accreditation Program
	Federal Election Commission Voting System Standards	VSS	April 2002	Federal Election Commission
	EAC Decision on Request for Interpretation 2007-04, 2005 VVSG Vol. 1 Section 3.1.3	Interpretation 2007-04	October 29, 2007	Election Assistance Commission
	EAC Decision on Request for Interpretation 2007-05, 2005 VVSG Vol. 1 Section	Interpretation 2007-05	November 6, 2007	Election Assistance Commission

Version #	Title	Abbreviation	Date	Author (Org.)
	4.2.1 (Testing Focus and Applicability)			
	EAC Decision on Request for Interpretation 2007-06, 2005 VVSG Vol. 1 Section 4.1.1, 2.1.2c &f, 2.3.3.3o and 2.4.3c&d. (Recording and reporting undervotes)	Interpretation 2007-06	November 7, 2007	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-01, 2002 VSS Vol. II, Section 4.7.1 & Appendix C 2005 VVSG Vol. II, Section 4.7.1 & Appendix C	Interpretation 2008-01	February 6, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-02, Battery Backup for Optical Scan Voting machines	Interpretation 2008-02	February 19, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-04, Ballot Production - Alternative languages	Interpretation 2008-04	May 19, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-05, Durability	Interpretation 2008-05	May 19, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-06 Battery Back Up for Central Count	Interpretation 2008-06	August 29, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-07 Zero Report	Interpretation 2008-07	August 27, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-08, Automatic Bar Code Reader	Interpretation 2008-08	August 1, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-09, Safety (NRTL)	Interpretation 2008-09	August 25, 2008	Election Assistance Commission
	EAC Decision on Request for Interpretation 2008-10 Electrical Fast Transient (EFT)	Interpretation 2008-10	August 26, 2008	Election Assistance Commission
	EAC Decision on VVPAT Accessibility	Interpretation 2009-01	October 5, 2009	Election Assistance Commission
	EAC Decision on Alternate Languages	Interpretation 2009-02	September 29, 2009	Election Assistance Commission
	EAC Decision on Batter Back Up for Central Count Systems	Interpretation 2009-03	September 28, 2009	Election Assistance Commission
	EAC Decision on Audit Log Events	Interpretation 2009-04	August 5, 2009	Election Assistance Commission
	EAC Decision on T-Coil Requirement	Interpretation 2009-05	June 25, 2009	Election Assistance Commission
	NOC 07-05: Voting System Test Laboratory (VSTL) responsibilities in the management and oversight of third party testing.	NOC 07-05	September 7, 2007	Election Assistance Commission
	NOC 08-001: Validity of Prior Non-core Hardware Environmental and EMC Testing	NOC 08-001	March 26, 2008	Election Assistance Commission
	NOC 08-002: EAC Mark of	NOC 08-002	May 16, 2008	Election Assistance

Version #	Title	Abbreviation	Date	Author (Org.)
	Certification Final			Commission
	NOC 08-003: Conformance Testing Requirements	NOC 08-003	July 30, 2008	Election Assistance Commission
	NOC 09-001: Requirements for Test Lab Development and Submission of Test Plans	NOC 09-001	May 1, 2009	Election Assistance Commission
	NOC 09-002: Laboratory Independence Requirement	NOC 09-002	May 4, 2009	Election Assistance Commission
	NOC 09-003: De Minimis Change Determination Requirements	NOC 09-003	September 18, 2009	Election Assistance Commission
	Voting System Testing and Certification Program Manual		1 January 2007	Election Assistance Commission
	Voting System Test Laboratory Program Manual		21 July 2008	Election Assistance Commission
	Sequoia Reuse of Hardware Testing Letter		24 July 2009	Election Assistance Commission
	Sequoia Reuse of Hardware Testing Letter		29 September 2009	Election Assistance Commission

1.3 *Technical Data Package Documents*

The Technical Data Package Documents submitted for this certification test effort are listed in Section 3 System Identification.

1.4 *Test Report Contents*

The contents of this Test Report include:

- Section 1: The Introduction - identifies the scope of certification testing.
- Section 2: The Certification Test Background identifies the process for the Physical and Functional Configuration Audits.
- Section 3: The Voting System Identification identifies the system configuration including hardware, software and the Technical Data Package documentation.
- Section 4: The Voting System Overview identifies the overall design and functionality of voting system.
- Section 5: The Certification Review and Test Results are the methods and results of the testing effort.
- Section 6: The Opinions & Recommendations of the acceptability of the voting system.

Test Operations, Findings and Data Analysis are in the appendices.

- Appendix A: Certification Test Requirements
- Appendix B: Source Code Reviews
- Appendix C: PCA TDP Document Reviews
- Appendix D: FCA Test Results
- Appendix E: Discrepancy Report
- Appendix F: Warrant of Accepting Change Control Responsibility
- Appendix G: Trusted Builds
- Appendix H: Amended Test Plan
- Appendix I: State Test Reports
- Appendix J: Sequoia Voting System Implementation Statement
- Appendix K: EAC Certification Number & Voting System Configuration

1.4.1 VSTL Program Manual Format Trace

Appendix B of the Voting *System Test Laboratory Program Manual v.1.0* identifies content in a specific format as does the Notice of Clarification (NOC) 09-004. The format of this report follows the recommended outline stipulated in the *VSS 2002* Vol. 2 Appendix B. As these documents indentify

placement of information in different locations a trace is being provided to clarify the location of the specified content in this report.

Table 3 Trace of the Test Report to the VSTL Program Manual and EAC NOC 09-004

EAC VSTL Program Manual Appendix B		Test Report - VSS 2002 *Vol.* 2 Appendix B	
1.	System Identification and Overview	1. 3. 4.	Introduction Voting System Identification Voting System Overview
2	Certification Test Background	2.	Certification Test Background
2.1	Revision History	2.	Certification Test Background
2.2	Implementation Statement	2. 7.9	Certification Test Background Implementation Statement
3 3.1	Test Findings and Recommendations Summary Finding and Recommendation	4.3.1.	Certification Review and Test Results Opinions & Recommendations
3.2	Reasons for Recommendation of Rejection	N/A	Not applicable; no recommendation of rejection
3.3	Anomalies (may also be identified as discrepancies, issues or defects)	Appendices: A B D E	Provides a general description of how anomalies were encountered and reported during testing. Appendix A traces the VSS requirements to the specific anomalies. Addendum to Appendix B contains software related source code discrepancy detail. Appendix D Tables: "Issues Opened" traces the specific anomalies to the relevant software build. Appendix E, PCA and FCA Discrepancy Report, provides the discrepancy number, date, tester, location, description, and *VSS 2002* requirement information about anomalies encountered during document reviews and testing.
3.4	Correction of Deficiencies	Appendices: A B D E	Provides a general description of how deficiency corrections were confirmed. Appendix A traces the VSS requirements to the specific closed anomalies. Addendum to Appendix B reflects pass criteria for all reviewed source code. Appendix D Tables: "Issues Closed" traces the specific anomaly resolutions to the build Appendix E, PCA and FCA Discrepancy Report, provides the vendor responses and resolution validations for anomalies encountered during document reviews and testing.
Appendix A	Additional Findings	Appendices: A D	Appendix A: Certification Test Requirements contains "should" and "not applicable" requirements. Comments provide rationale and references to relevant EAC Interpretations or Notices of Clarification. Appendix D: Supported Voting Variations of the *VSS 2002* Section 2.2.8.2 identifies "unsupported" optional functionality.
Appendix B	Warrant of Accepting Change Control Responsibility	Appendix F	Warrant of Accepting Change Control Responsibility
Appendix C	Witness Build	Appendix G	Trusted Build and Validation Tools documents the Witness of the Trusted Build

EAC VSTL Program Manual Appendix B		Test Report - VSS 2002 *Vol.* 2 Appendix B	
Appendix D	Test Plan	Appendix H	Test Plan
Appendix E	State Test Reports	Appendix I	State Test Reports
		Appendix J	Implementation Statement
		Appendix K	EAC Certification Number

2 Certification Test Background

Earlier versions of products in this effort completed qualification testing under the outdated NASED program. These earlier versions are in use, as permitted under the laws of the various states. Under the EAC program, all systems submitted must be fully tested as a new system. As such the WinEDS 4.0 Certification test campaign is an initial certification to the *2002 VSS*.

As part of their application for Certification Testing, Sequoia Voting Systems submitted their implementation statement (see Section 7.10) for the WinEDS 4.0 voting system. Certification testing of the Sequoia WinEDS 4.0 voting system included a Physical Configuration Audit and a Functional Configuration Audit. Daily status reports were sent to Dominion certification management staff and iBeta project test staff. These reports included project activity status, issues, and other relevant information. Weekly status calls were held with the EAC, EAC Reviewers and Dominion. Upon request, iBeta provided the EAC with information to clarify the testing, test process, schedule, and interim discrepancy reports.

2.1 *Terms and Definitions*

The Terms and Definitions identified below are used in this test report.

Table 4 Terms and Definitions

Term	Abbreviation	Definition
Detachable Audio Voting Control (ABLE-D)	ABLE-D	Audio voting control for the EDGE2*plus* which provides blind, dexterity challenged Voters and Voters with reading limitations an easy way to vote independently, using an Audio or a Sip & Puff interface. It can be detached from the base unit, attached only by its coiled power/data cord.
APS External Printer (Model UTG300)	UTG	APS External Printer, which is used to print and physically record votes and provide election reports for the EDGE2*plus* (this component is not part of the certified voting system)
Audit Trail Memory	Audit Trail Cartridge	Removable memory cartridge, which contains an unalterable randomized electronic record of all votes cast during an election. Identical data is stored on the Results Cartridge for the voting system. If an Audit Trail Cartridge is present in the aux port, the event log data will be written there as well.
AVC Edge	Edge II	Sequoia Voting Systems' stand-alone DRE polling place voting machine that incorporates a color LCD integral touch screen, integrated (voter) privacy flaps, poll worker panel, internal memory for storing ballot data and voting records, removable results cartridge, and protective & public counters.
Card Activator	Card Activator	A component of the AVC Edge that serves as the voter's access to the AVC Edge (Edge II) direct-record electronic touch-screen voting system by use of a Smart Card (aka Voter Card).
Direct Recording Electronic	DRE	An electronic voting system that utilizes electronic components for the functions of ballot presentation, vote capture, vote recording, tabulation and logically & physically integrated into a single unit.

Term	Abbreviation	Definition
Edge Audio Voting Accessory	E-AVA	The audio voting device provides an unassisted, private & secure voting experience for the visually impaired. The voter listens to a spoken audio presentation of the ballot while using the audio voting device to navigate through the ballot and cast their vote.
Edge Aux Power Unit		Provides emergency power for up to two AVC Edge for a minimum of two hours.
EDGE2*plus* Model 300	EDGE2*plus*	Sequoia Voting Systems' stand-alone DRE polling place voting machine that incorporates a color LCD integral touch screen, integrated (voter) privacy flaps, poll worker panel, internal memory for storing ballot data and voting records, removable results cartridge, and protective & public counters. There are three configurations submitted for federal certification (CO.3, 305 and CO.4).
EDGE2*plus* USB K9K Cartridges	Cartridges (USB)	COTS K9K Series USB format flash memory drives used as Results, Audit Trail, or Vote Simulation cartridges.
Election Management System	EMS	Ballot preparation and central count functionality of a voting system
Endorsed Candidates		Used in NJ, NY, NYC, and PA. A Candidate that is endorsed by their own political party along with that of a different political party.
Escrow Agency		EAC identified repository that retains the file signature of the trusted build
Help America Vote Act	HAVA	Legislation enacted in 2002 which includes creation of the EAC, federal voting standards and accreditation of test labs
Hybrid Activator, Accumulator & Transmitter Unit Model 50	HAAT50	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT50 does not consolidate, print or transmit results. There are two configurations submitted for federal certification (v 0.3 and v 1.1)
Hybrid Activator, Accumulator & Transmitter Unit Model 80	HAAT80	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT80 also serves as a precinct level accumulator for consolidating and printing the consolidated results. The HAAT 80 does not transmit.
Hybrid Activator, Accumulator & Transmitter Unit Model 90	HAAT90	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT90 serves as a precinct level accumulator for consolidating and printing the consolidated results and for transmission of unofficial results over fixed telephone line networks to a central tally server.
Hybrid Activator, Accumulator & Transmitter Unit Model 100	HAAT100	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT100 serves as a precinct level accumulator for consolidating and printing the consolidated results and for transmission of unofficial results from all precinct voting devices over CDMA 1X secured networks to a central tally server.

Term	Abbreviation	Definition
Insight Battery		12 VDC battery which provides emergency power for an Optech Insight during power failures
Insight Memory Pack Reader	IMPR	The IMPR device attaches to the HAAT80, 90, and 100 via a serial port interface. It is used for reading Insight results.
Log Printer		COTS printer connected to the Optech 400-C LP2 port used for log printing.
Memory Cartridge		COTS ATA/PCMCIA flash memory for the AVC Edge 5.1.
Memory Pack Receiver	MPR	The MPR device attaches to a WinEDS workstation and is used to create Insight memory packs and read results.
Memory Pack		Removable cartridge containing election parameter data, precinct totals, electronic log data and optional CVR data used by the Optech Insights.
Official Operating Mode		The operating mode used on election day. Vote simulation cannot be performed in the Official mode. Pre-LAT and Post-LAT results cannot be intermixed or accumulated with votes cast in the Official Operating Mode.
Optech 400-C	Sequoia 400-C	Sequoia Voting Systems' central count ballot tabulator that reads ballots, tabulates the results and prepares output reports.
Optech Insight		A portable Precinct Count System that uses Optical Scan Read-Head technology to electronically read and tabulate Optical Scan ballots at the Polling Place, print results and store election totals.
Optech Insight Plus		Same as the Optech Insight, with the addition of an LCD panel display and a ready light.
Plain Old Telephone Service	POTS	Terminology used to refer to analog voice-quality telephone service used by some types of telecommunications. The abbreviation is used especially to distinguish it from any digital telephone system.
Political Subdivisions	PSD	A geopolitical unit whose voters vote for one or more offices. One or more precincts (or parts of precincts) are included in a PSD.
Post-election logic and accuracy testing	Post-LAT	Post-LAT mode is used after the election to confirm the vote recording accuracy results match Pre-election LAT results. Vote simulation can be used in Post-LAT mode. Post-LAT mode votes cannot be intermixed or accumulated with Official Mode results.
Pre-election logic and accuracy testing	Pre- LAT	Pre-LAT mode is used for validating accurate vote recording accuracy prior to an election. Vote simulation can be used in Pre-LAT mode. Pre-LAT mode votes cannot be intermixed or accumulated with Official Mode results.
Primary – Closed		Voters must declare a party affiliation in order to vote in the primary. The voter declares their party affiliation to the election official and receives a ballot containing only those party-specific contests, along with non-party-specific contests presented at the same election. Unaffiliated voters are permitted to vote only on non-party-specific contests.

Term	Abbreviation	Definition
Primary – Open (Selective or Pick-A-Party)		Voters do not have to declare a party affiliation in order to vote in the primary. Depending on state law, the voter can declare their party preference to the election official or make their choice of party within the privacy of the voting booth. The voter receives a ballot containing only those party-specific contests, along with non-party-specific contests presented at the same election. Unaffiliated voters are permitted to vote only on non-party-specific contests.
Primary – Open		Voters do not have to declare a party affiliation in order to vote in the primary. A primary election (aka Top Two) that allows voters to choose among all candidates running for each office. Candidates from all parties are listed under the same contest.
Remote Access Server	RAS	Analog (POTS) telephone endpoint at Central Count for a HAAT90 transmission.
Report Printer		COTS printer connected to the Optech 400-C LP1 port used for report printing.
Results Cartridge		Removable memory cartridge for a DRE containing the ballot, election results and audit log
Seiko DPU-414 Printer	Seiko Printer	A 40-column dot matrix printer, which is used to provide election reports for the AVC Edge.
Simulation Cartridge	Vote Simulation	Removable memory cartridge containing a vote simulation script. This is a configuration option for Pre-LAT and Post-LAT operating modes.
Sip & Puff device	Sip & Puff	A DRE ballot navigation and vote selection assistive device, used by individuals with dexterity challenges or limitations on the use of their hands
Smart Card		Same as Voter Card. Card issued by the poll worker to be used as a key to access the ballot on the DRE voting machines for voting purposes.
Technical Data Package	TDP	The documentation and code relating to the voting system, submitted by the manufacturer for review by the VSTL.
Training Mode		Training Mode is used for poll worker training and allows voting in an Official Training Mode as indicated on the DRE. This mode allows multiple passes through Official Election mode.
U.S. Election Assistance Commission	EAC	U.S. agency established by the Help America Vote Act of 2002 to administer Federal elections.
VeriVote Printer		Sequoia Voting Systems' side-mounted VVPAT printer for an AVC Edge DRE.
Voluntary Voting System Guidelines	VVSG	Federal voting system test standard revision stipulated by HAVA.
Voter Card		Card issued by the poll worker to be used as a key to access the ballot on the DRE voting machines for voting purposes.
Voting System Standards	VSS	Federal voting system test standards, predecessor of the VVSG.
Voting System Test Lab	VSTL	Lab accredited by the EAC to perform certification testing of voting systems.

Term	Abbreviation	Definition
Voting Variations		Significant variations among state election laws incorporating permissible ballot content, voting options and associated ballot counting logic
Voter Verified Paper Audit Trail	VVPAT	A software independent printed record of the electronic DRE ballot cast which is to be confirmed by the voter as an accurate report of their vote
Windows Election Data System	WinEDS	A client/server election management application for ballot preparation and central count consolidation and reporting of the Election Management of the Sequoia Voting Systems voting system. This system also includes Extended Services and Election Reporting.
WinEDS/HAAT Listener		A server-based application designed to receive encrypted unofficial electoral data and, optionally, configuration data and event logs, from previously authorized transmitting HAAT devices and validates the integrity of all data received, and stores it in a centralized database management system (DBMS). HAAT devices can also use the WinEDS/HAAT Listener server to synchronize their time and date with that of the server, so all HAAT devices will have an approximately similar time.
WinETP		Election Tabulation software Program that enables the Optech 400-C to tabulate ballots and report results.

2.2 *Physical Configuration Audit*

The Physical Configuration Audit (PCA) deals with the physical elements of the voting system, including the source code, documentation and system configuration reviews. Validation of COTS software and hardware, execution of a Trusted Build with the reviewed source code and installation of the executables are part of the PCA.

2.2.1 PCA TDP Source Code Review

The PCA TDP Source Code Review of Sequoia WinEDS 4.0 was performed to verify conformance to the *VSS 2002* Vol. 1 Section 4.2 and Vol. 2 Section 5. Reviewed results were recorded on Source Code Review sheets (Excel spreadsheets). Issues were identified in the review and logged on a Discrepancy Report, after completion of peer review. The Discrepancy Report was forwarded to Dominion for correction.

2.2.2 PCA TDP Document Review

The PCA TDP Document Review of Sequoia WinEDS 4.0 performed to verify conformance to Vol. 2 Section 2 of the *VSS 2002*. Reviewed results are recorded on PCA TDP Document Review sheets (Excel spreadsheets). Issues were identified in the review and logged on a Discrepancy Report, after completion of peer review. The Discrepancy Report was forwarded to Dominion for correction.

2.2.3 PCA System Configuration Review

The PCA System Configuration Review of Sequoia WinEDS 4.0 was performed to verify conformance to the VSS Vol. 1 Section 8.7.1. Reviewed results are recorded on PCA System Configuration Review sheets (Excel spreadsheets). Issues were identified in the review and logged on a Discrepancy Report, after completion of peer review. The Discrepancy Report was forwarded to Dominion for correction.

2.2.4 Witness, Trusted Build and Installation

The Witness Build and Installation of the executable code for Sequoia WinEDS 4.0 was performed using the review source code per the VSS Vol. 1 Section 9.6.2.4. Observation of the build was

documented in the Witness of the Final Build and Code Comparison Template (Word Document). Trusted builds were conducted in accordance with the requirements of the EAC Certification and Program Manual.

2.3 *Functional Configuration Audit*

The Functional Configuration Audit was an examination of the functional aspects of the voting system. This included review of the Sequoia WinEDS 4.0 submitted test documentation and execution of all required tests. An audit was also performed at the vendors' offices that consisted of a review of Quality Assurance and Configuration Management policies and practices. The review of the vendor testing was conducted as well and this review indicated a deficiency in the testing of the audit logs. As a result iBeta focused test cases on testing and validating the audit logs.

2.3.1 FCA Test Documentation Review

The FCA Test Documentation Review assessed the level of vendor testing of the voting system to the VSS Vol. 1 Section 2, 3, 5, 6, and 8 requirements. This assessment was used to define the extent of functional testing.

2.3.2 FCA Functional, Accessibility, Maintainability, and Reliability Tests

Functional and System Level Tests were conducted, in accordance with Vol. 2 Section 6. End-to-end mock elections were conducted to demonstrate the integrated functionality and processes of the Sequoia WinEDS 4.0 voting system. Upon completion of these Functional and System Level test cases, the evaluation of the Sequoia WinEDS 4.0 voting system was found to meet the accessibility requirements of the *VSS 2002, Section 2.2.7 a) through e).*

The system configuration, test objective, test steps, and expected results were identified in each test case. Acceptance and rejection results were recorded for each test step. Issues encountered during testing were identified in the test record and logged on *PCA and FCA Discrepancy Report*, after completion of peer review. Dominion resolved all discrepancies which did not meet the requirements of the *VSS 2002*. Tests were rerun to validate all submitted fixes and these validations were recorded in the *PCA and FCA Discrepancy Report*.

2.3.3 FCA Volume, Stress, Data Accuracy, and Error Recovery Tests

iBeta reviewed the Sequoia's *Practical System Limits* (as submitted to the EAC as part of the Implementation Statement) to identify relevant application and system limits. Based upon the system and application limits identified in this document iBeta defined and conducted a set of two test cases. These test cases incorporated end-to-end mock elections to demonstrate the ability of the system to operate at the declared limits. Additional scenarios were incorporated into the test cases to demonstrate the system's ability to provide an appropriate response to an overloading conditions exceeding the limits and recover without losing vote data.

The Data Accuracy *VSS 2002* requirements for the vote counting components of WinEDS were tested within two Data Accuracy Volume Test Cases. Any issues encountered during testing were identified in the test record and logged on a *PCA and FCA Discrepancy Report*, after completion of peer review. Sequoia resolved all discrepancies which did not meet the requirements of the *VSS 2002*. Tests were rerun to validate all submitted fixes.

2.3.4 FCA Security Tests

iBeta performed a security review of the Sequoia security documentation addressing Vol. 1 Section 2.2.1, 2.2.3, 2.2.5 and 6 and Vol. 2 Section 6.4. Based upon this review security specific tests were identified. In additional to functional and system level tests, these tests incorporated source code and document reviews. Functionality to meet the requirements incorporated secrecy, integrity, system audit, error recovery or access to the voting system. The review was either conducted or peer reviewed by an iBeta CISSP staff member. The tests or reviews to validate the security of WinEDS 4.0 were recorded in the *FCA Security Review*. Sequoia resolved all discrepancies which did not meet the requirements of the *VSS 2002*. Tests were rerun to validate all submitted fixes.

2.3.5 FCA Hardware Environmental Tests

FCA Hardware Environmental Tests are non-core tests which must be performed by a laboratory accredited in the hardware environmental test methods identified in *VSS 2002 Vol.*1, 4.6 and 4.7. Non-core tests may be performed by subcontractor laboratories, under the supervision of the VSTL, if the VSTL does not hold these accreditations. iBeta validated Criterion Laboratories, Wyle Laboratory, and APT (Oracle) accreditation to perform all required hardware environmental tests and engaged them as iBeta's subcontractors to perform the tests.

During the initial assessment of the Sequoia WinEDS 4.0 voting system hardware, iBeta reviewed the previous testing from the NASED certification test effort where FEC Voting System Standards 2002 were utilized and testing was performed by Criterion, Percept Technologies, and Wyle Labs in accordance with the EAC NOC 08-001 for test result reuse with the following conditions being met:

- The hardware was unchanged and the laboratory that performed the testing verified in an independent assessment that the equipment they tested was essentially the same as the system tendered for this test campaign; and
- iBeta confirmed that Criterion Technology Corp, Percept Technology and Wyle Laboratories were accredited by A2LA to perform all the *VSS 2002* required test methods accredited in the test methods they performed on the date of test execution.

Subsequent to that initial assessment and prior to completion of all hardware testing, Sequoia petitioned the EAC for hardware test results reuse from the previous NASED certification test effort and received written approval for the additional reuse of previous NASED hardware test results as documented in the EAC letters to Sequoia dated 24 July 2009 and 29 September 2009.

Based on the testing remaining, a detailed test case with test instructions was provided to third party test labs to review, assess and test the Sequoia WinEDS 4.0 voting system. iBeta created test election databases for all operating tests and to validate the operational status of the Sequoia WinEDS 4.0 voting system before and after each environmental test. The system configuration, test objective, test steps, and expected results were identified. Acceptance and rejection results were recorded for each test step. Issues encountered during testing were documented in the test record. In addition to the iBeta test record, each third party lab provided iBeta with anomaly and test reports following their internal processes. iBeta logged anomaly reports as issues on the *PCA and FCA Discrepancy Report.* Sequoia resolved all discrepancies which did not meet the requirements of the *VSS 2002.* EAC Interpretation 2007-05 provided that there is no merit to the interpretation that requires FCA Hardware Environmental testing of unmodified COTS equipment. Instead the interpretation requires the confirmation of FCC Class 15B and CE marks affixed to each unit indicating that the COTS product has been certified to meet those standards and a copy of the COTS manufacturer's Declaration of Conformity confirming the manufacturer's compliance claim. iBeta followed the interpretation for the Sequoia WinEDS 4.0 voting system.

2.3.6 FCA Telephony and Cryptographic Review and Tests

An examination of the Sequoia WinEDS 4.0 voting system was conducted to confirm that it does contain both landline and wireless data interchange devices. The results of this review were recorded in the *FCA Telephony and Cryptographic Test Case.* Based upon this review specific tests were identified against the requirements of VSS Vol. 1 Section 5 and 6. Functionality to meet the requirements incorporated telephony and cryptography of the voting system. The testing and review was either conducted or peer reviewed by an iBeta CISSP staff member. The tests or reviews to validate the security of WinEDS 4.0 were recorded in the *FCA Security Review.* Sequoia resolved all discrepancies which did not meet the requirements of the *VSS 2002.* Tests were rerun to validate all submitted fixes.

3 Voting System Identification

The description of the Sequoia WinEDS 4.0 submitted for certification is found in the EAC Scope of Certification as noted in Section 3.1. The hardware, software and the Technical Data Package documentation used in the certification test environment is identified in Section 3.2.

3.1 *Submitted Voting System Identification*

Table 5 Voting System Name and Version

Voting System Name	Version
Identified in the EAC Scope of Certification	

Table 6 Voting System Polling Place and Central Count Hardware

Hardware	OS or Firmware & Version	Description
Identified in the EAC Scope of Certification		

Table 7 Voting System EMS Software

Software Applications	Version	EMS Function Description
Identified in the EAC Scope of Certification		

3.2 *Voting System Test Environment*

The Voting System Test Environment identifies the specific hardware and software that was used in the test environment. The Test Methods in Appendix D identify the specific WinEDS 4.0 voting system software and firmware build installed for each test iteration.

Table 8 Voting System Hardware

Hardware	OS or Version	Manufacturer	Description
Ballot Prep & Central Count			
EMS Configuration – HAAT90			
WinEDS 4.0 Workstation: Optiplex 330 Intel Pentium Dual CPU 1.60GHz, 0.98GB of RAM	Windows XP Pro SP2	Dell	DRE ballot preparation and optical scan ballot programming PC (WinEDS 4.0) used in conjunction with the HAAT90.
WinEDS 4.0 Server: PowerEdge 1900 Intel Xeon CPU 1.60GHz, 1.99GB of RAM	Windows Server 2003 R2	Dell	DRE ballot preparation and optical scan ballot programming PC (SQL Server) and central count used in conjunction with the HAAT90.
HAAT Listener: Dell PowerEdge 2900 Intel Xeon CPU 1.60GHz, 0.98GB of RAM	SUSE 10 Linux Enterprise SP1	Dell	Central count HAAT Listener server used in conjunction with the HAAT90 election data transmissions.
RAS Server: Dell PowerEdge 840 Intel Pentinum Dual CPU 2.13GHz, 2.50GB of RAM	SUSE 10 Linux Enterprise SP1	Dell	Central Count Remote Access Server used in conjunction with the HAAT90 dial-in election data transmissions.
Hybrid Activator, Accumulator & Transmitter Unit Model 90	A1.1	Sequoia Voting Systems	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT90 serves as a precinct level accumulator for consolidating and tallying results, a thermal printer for printing the results and for transmitting unofficial results over fixed telephone line networks to central tally server.
Insight Memory Pack Reader (IMPR)	A1.0	Sequoia Voting Systems	Serial Port interface for the HAAT80, 90, and 100 to read Insight MemoryPacks.
Watchguard Firebox 750e	XTM 11.1	Watchguard	Firewall and IPS for HAAT90

Hardware	OS or Version	Manufacturer	Description
			transmissions
EMS Configuration – HAAT100			
WinEDS 4.0 Workstation: Optiplex 330 Intel Pentium Dual CPU 1.60GHz, 0.98GB of RAM	Windows XP Pro SP2	Dell	DRE ballot preparation and optical scan ballot programming PC (WinEDS 4.0) used in conjunction with the HAAT100.
WinEDS 4.0 Server: PowerEdge 1900 Intel Xeon CPU 1.60GHz, 1.99GB of RAM	Windows Server 2003 R2	Dell	DRE ballot preparation and optical scan ballot programming PC (SQL Server) and central count used in conjunction with the HAAT100.
HAAT Listener: Dell PowerEdge 2900 Intel Xeon CPU 1.60GHz, 0.98GB of RAM	SUSE 10 Linux Enterprise SP1	Dell	Central Count HAAT Listener used in conjunction with the HAAT100 wireless election data transmissions.
Hybrid Activator, Accumulator & Transmitter Unit Model 100	A0.7	Sequoia Voting Systems	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT100 serves as a precinct level accumulator for consolidating and tallying results, a thermal printer for printing the results and for transmission of unofficial results from all precinct voting devices over CDMA 1X/TLS secured networks to a central tally server.
Insight Memory Pack Reader (IMPR)	C1.1	Sequoia Voting Systems	Functionality the same as the IMPR A1.0 except for 3 minor hardware changes.
Watchguard Firebox 750e	XTM 11.1	Watchguard	Firewall and IPS for HAAT100 transmissions
EMS Configuration – General			
WinEDS 4.0 Workstation/Server: Dell Lattitude 630 Intel Pentium Dual CPU 2.49GHz, 3.50GB of RAM	Windows XP Pro SP2	Dell	DRE ballot preparation, optical scan ballot programming PC (WinEDS 4.0) and central count (SQL) server.
WinEDS 4.0 Workstation/Server: Dell Lattitude 610 Intel Pentium 1.86GHz Processor 781 MHz, 504 MB RAM	Windows XP Pro SP2	Dell	DRE ballot preparation, optical scan ballot programming PC (WinEDS 4.0) and central count (SQL) server.
WinEDS 4.0 Workstation/Server: Dell Lattitude 620 Intel Pentium Dual CPU 2.49GHz, 3.50GB of RAM	Windows XP Pro SP2	Dell	DRE ballot preparation, optical scan ballot programming PC (WinEDS 4.0) and central count (SQL) server.
Hybrid Activator, Accumulator & Transmitter Unit Model 50	A0.3	Sequoia Voting Systems	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface.
Hybrid Activator, Accumulator & Transmitter Unit Model 50	A1.1	Sequoia Voting Systems	Functionality the same as HAAT Model 50 except for 7 hardware changes.
Hybrid Activator, Accumulator & Transmitter Unit Model 80	A1.1	Sequoia Voting Systems	A Sequoia Voting Systems' component that provides voter access to the DREs through activation of a Voter/Smart Card interface. The HAAT80 also serves as a precinct level accumulator for consolidating and tallying results and a thermal printer for printing the results
MemoryPack Receiver (MPR)	Rev E	Sequoia Voting Systems	A desktop device, which is connected to a PC via COM port

Hardware	OS or Version	Manufacturer	Description
			which was developed specifically to work in conjunction with WinEDS 4.0 (Windows Election Database System) installed on a PC, to encode precinct election data from WinEDS 4.0 to a MemoryPack.
Voter/Smart Card		COTS	Card issued by the poll worker to be used as a key to access the ballot on a DRE for voting purposes.
Optech 400-C			
Optech 400-C	3.02P	Sequoia Voting Systems	Sequoia Voting Systems' central count ballot tabulator that reads marked ballots, tabulates and prepares output reports.
Desktop Personal Computer Intel Celeron 2 - 2.53 GHz RAM: 256 MB	Dimension 1100	Dell	Personal computer that runs the WinETP 1.16 application for the Optech 400-C.
USB Flash Drive		COTS	COTS removable flash memory for WinETP file transfers (to/from WinEDS).
Polling Place			
DRE – Edge II			
AVC Edge (Edge II)	5.2	Sequoia Voting Systems	Sequoia Voting Systems' stand-alone touch screen DRE polling place voting device that incorporates a color LCD integral touchscreen, poll worker panel, integrated (voter) privacy flaps, internal memory for storing ballot data and voting records, removable Results Cartridge, and protective & public counters.
VeriVote Printer	Rev C	Sequoia Voting Systems	Sequoia Voting Systems' optional side-mounted VVPAT printer to an AVC Edge 5.2 machine, to produce a paper record that can be reviewed by the Voter during the voting process.
Seiko Printer	DPU-414	Seiko	A COTS 40-column dot matrix printer, which is used to provide election reports for the AVC Edge 5.2.
Edge Audio Voting Accessory (E-AVA)	Rev D	Sequoia Voting Systems	A six button device designed for use with the AVC Edge 5.2 that allows unassisted, private & secure voting for the visually impaired and non-reading voters using a spoken, audio ballot format.
Edge Aux Power Unit	BTC80W	Lien Engineering	COTS emergency power unit that provides power for two AVC Edges for an extended period of time.
Card Activator	Rev D & E	Sequoia Voting Systems	A component of the AVC Edge 5.2 that serves as the voter's access to the AVC Edge 5.2 direct-record electronic touch-screen voting system by use of a Voter/Smart Card.
Memory Cartridge	ATA/PCMCIA	COTS	COTS removable flash memory for the AVC Edge 5.2.
DRE – EDGE2*plus*			
EDGE2*plus* Model 300	CO.3	Sequoia Voting Systems	Sequoia Voting Systems' stand-alone touch screen DRE polling place voting device that incorporates

Hardware	OS or Version	Manufacturer	Description
			an LCD voter display panel, poll worker panel, integrated (voter) privacy flaps, internal memory for storing ballot data and voting records, removable Results Cartridge, protective & public counters, an ABLE-D audio voting control and APS external printer VVPAT (UTG) .
EDGE2*plus* Model 300	CO.4	Sequoia Voting Systems	Same as EDGE2*plus CO.3 except* for changes (including the change of the LCD) reflected in Change Order 4 (CO.4).
EDGE2*plus* Model 305	CO.4	Sequoia Voting Systems	Same as EDGE2*plus CO.4 except* without the ABLE-D audio voting control.
APS External Printer	UTG300	Advanced Printing Systems (APS)	Optional COTS side-mounted 40-column election report VVPAT thermal printer for the EDGE2*plus*.
Detachable Audio Voting Control (ABLE-D)	N/A	Sequoia Voting Systems	An eight-button device integrated into and designed for use with the EDGE2*plus* Model 300 that provides unassisted, private and secure voting for visually impaired, non-reading and voters with dexterity challenges or limitations on the use of their hands.
Results USB Cartridge	Series 700/800	COTS Series K9K	COTS USB flash drive used to capture Election Day ballot, results & audit log
Simulation USB Cartridge	Series 700/800	COTS Series K9K	COTS USB flash drive used to simulation script used for Pre and Post Election Logic & Accuracy Test mode
Audit Trail USB Cartridge	Series 700/800	COTS Series K9K	COTS USB flash drive used to contain unalterable randomized electronic record of all votes cast during an election.
Optical Scanners			
Optech Insight	G.05	Sequoia Voting Systems	A portable Precinct Count System that uses Optical Scan Read-Head technology to electronically read and tabulate Optical Scan ballots at the Polling Place, print results and store election totals.
Optech Insight Plus	A.05	Sequoia Voting Systems	Same as the Optech Insight, with the addition of an LCD panel display.
MemoryPack	Rev C	Sequoia Voting Systems	Removable cartridge containing election parameter data, precinct totals, electronic log data and optional CVR data used for the Optech Insights.
Insight Battery	PS 12180 F2	Powersonic	COTS 12 VDC battery which provides emergency power for an Optech Insight or Insight Plus during power failures

Table 9 Voting System Software

Software Ballot Prep & Central Count	Version	Manufacturer	Identify Hardware
EMS Software			Ballot preparation/Central Count
WinEDS Election Management System	4.0.175	Sequoia Voting Systems	DRE ballot preparation, optical scanner programming & central count EMS software
Extended Services	1.0.81	Sequoia Voting Systems	A suite of common services and features for ballot preparation, programming, and central count
Election Reporting	4.0.73	Sequoia Voting Systems	Election Reports and flat file exports providing election night tally, historical summary data repository, and additional reporting capabilities
Memory Pack Receiver	3.01.080422.0552	Sequoia Voting Systems	Firmware for the MPR (peripheral device connected via serial interface to a WinEDS workstation), that reads from and writes to Insight memory packs.
Central Count Software			
WinETP	1.6.15	Sequoia Voting Systems	Central count EMS software for the 400-C
HAAT Listener	1.7.4	Sequoia Voting Systems	Central count software to receive election results transmitted from the HAAT90 or HAAT100
Polling Place			
DRE			
AVC Edge	5.2.16	Sequoia Voting Systems	Edge II polling place firmware.
VeriVote	1.04	Sequoia Voting Systems	Edge II VVPAT polling place software.
Edge Audio Unit	8.7.7	Sequoia Voting Systems	Edge II E-AVA polling place firmware to support audio ballots.
Card Activator	5.2.6	Sequoia Voting Systems	Edge II polling place software to program voter activation Smartcards
EDGE2*plus*	1.2.74	Sequoia Voting Systems	EDGE2*plus* polling place firmware.
HAAT (50, 80, 90, 100)	2.6.34	Sequoia Voting Systems	Polling place software to activate Vote session Smartcards for the DREs (HAAT50, 80, 90, & 100), accumulate, print results (HAAT80, 90, & 100), and transmit results (HAAT90 wired & 100 wireless).
Optical Scanner			
Insight/Insight Plus (HPX)	L1.46.100205.1100	Sequoia Voting Systems	Insight and Insight Plus polling place firmware that scans and reads paper ballots on the Insight scanners
Insight Memory Pack Receiver (IMPR)	2.14	Sequoia Voting Systems	Polling place software to read MemoryPacks used by the Insight optical scanners and transfers election results to the HAAT80, 90, and 100.
MemoryPack (APX)	L2.18.100205.1359	Sequoia Voting Systems	Polling place firmware directing the movement and operations of paper ballots through the Insight optical scanners

Table 10 Voting System Technical Data Package Documents

File Name	Document Title	Revision	Doc Date
Note: The Author of all the following documents is Sequoia Voting Systems (SVS)			
Voting System Wide Documents			
4-0_Voting_System_Environment_Hardening.pdf	4.0 Voting System Environment Hardening	A.22	Aug 2010
Implementation_Statement.pdf	Implementation Statement Release 4.0	A.14	Jul 2010
System40_Firmware_Build_Notes.doc	System 4.0 Firmware Build Notes	1.07	Jul 2010
AVC EDGE Documents			
CardAct_OpMaint.doc	Card Activator Operator's And Maintenance Manual 5.2	1.15	Jul 2010
EDGE_APU_OpMaint.doc	Edge Aux Power Unit Operator's And Maintenance Manual 5.2	1.10	Jun 2010
EDGE_AVA_PollWorkerOp.doc	Edge Audio Voting Accessory Poll Workers And Operators Manual	1.09	Aug 2010
EDGE_APL.doc	AVC Edge Approved Parts List 5.2	1.09	Jun 2010
EDGE_ChgRelSummary.doc	AVC Edge Change Release Summary 5.2	1.05	Jun 2010
EDGE_CMPlan.doc	AVC Edge Configuration Management Plan 5.2	1.09	Jun 2010
EDGE_FEC-XRef.doc	Trace To Vendor Testing And Technical Data Package	1.16	Jun 2010
EDGE_FunctSpec.doc	AVC Edge Functional Specifications	1.09	Jun 2010
EDGE_HardSpec.doc	AVC Edge Hardware Specification	1.09	Jun 2010
EDGE_MaintMan.doc	AVC Edge Maintenance Manual 5.2	1.11	Jun 2010
EDGE_OpMan.doc	AVC Edge Operators Manual 5.2	1.20	Aug 2010
EDGE_PersTraining.doc	AVC Edge Personnel And Training Requirements 5.2	1.07	Jun 2010
EDGE_PollWorker.doc	AVC Edge Poll Workers Manual	1.10	Jun 2010
EDGE_QAProgram.doc	AVC Edge Quality Assurance Program	1.09	Jun 2010
EDGE_SampleReports.doc	AVC Edge Sample Reports	1.07	Jun 2010
EDGE_Security.doc	AVC Edge Security Specification 5.2	1.12	Jul 2010
EDGE_SoftSpec.doc	AVC Edge Software Specification 5.2	1.14	Aug 2010
EDGE_SysOverview.doc	AVC Edge System Overview 5.2	1.11	Jun 2010
EDGE_TDP.doc	AVC Edge Technical Data Package	1.09	Jun 2010
EDGE_TestVerifSpec.doc	AVC Edge Test And Verification Specification	1.07	Jun 2010
EDGE_Penetration.doc	A AVC Edge Security Specification, Appendix B: Penetration Analysis 5.2	1.03	Sep 2009
VP_OpMaint.doc	VeriVote Printer Operator's And Maintenance Manual	1.20	Jun 2010
EDGE2*plus* Documents			
P168_Controller_Trusted_Build.doc	P168 Controller Trusted Build Guide	1.09	Jul 2010
E2P_Application_Compilation	EDGE2plus Application Compilation	1.14	Jul 2010
TSM_Player_Compilation.doc	EDGE2plus TSM Player Compilation Process	1.6	Jun 2010
E2P_OS_Creation.doc	Edge2plus Operating System Image Creation Process	1.16	Jun 2010
Edge2plus_CMPlan.doc	EDGE2PLUS MODEL 300 Configuration Management Plan	3.10	Jun 2010
Edge2plus_FactoryDiagnostics.doc	EDGE2PLUS MODEL 300 DIAGNOSTICS APPLICATION MANUAL	3.09	Jun 2010
Edge2plus_FECXRef.doc	Trace to Vendor Testing and Technical Data Package	3.10	Jun 2010
Edge2plus_FunctSpec.doc	EDGE2PLUS MODEL 300 FUNCTIONAL SPECIFICATION	3.09	Jun 2010
Edge2plus_HardSpec.doc	Edge2plus Model 300 Hardware Specification	3.11	Jun 2010
Edge2plus_MaintMan.doc	Edge2plus Model 300 Maintenance Manual	3.10	Jun 2010
Edge2plus_OpMan.doc	Edge2plus Model 300 Operator's Manual	3.15	Aug 2010
EDGE2plus_Penetration.doc	EDGE2*plus* Security Specification Appendix B Penetration Analysis	1.0	Nov 2009

File Name	Document Title	Revision	Doc Date
Edge2plus_PersTraining.doc	EDGE2PLUS MODEL 300 PERSONNEL & TRAINING REQUIREMENTS	3.04	Jun 2010
Edge2plus_QAProgram.doc	Edge2plus Model 300 Quality Assurance Program	3.06	Jun 2010
Edge2plus_Security.doc	Edge2plus Model 300 Security Specification	3.12	Jun 2010
Edge2plus_SoftSpec.doc	Edge2plus Model 300 Version C03 Software Specification	3.13	Jun 2010
Edge2plus_SysOverview.doc	Edge2plus Model 300 System Overview	3.08	Jun 2010
Edge2plus_TDP.doc	Edge2plus Model 300 Technical Data Package	3.05	Jun 2010
Edge2plus_TestVerifSpec.doc	Edge2plus Model 300 Test & Verification Specification	3.08	Jun 2010
Edge2plus_APL_C04.doc	Edge2plus Model 300™ Revision C0.4 Approved Parts List	3.07	Jun 2010
ABLE-D_OpMan.doc	Able-D (Detachable Audio Voting Control) Operators Manual	3.05	Jun 2010
Edge2plusC03_APL.doc	Edge2plus Model 300 version C0.3 Approved Parts List	3.04	Jun 2010
HAAT Overview Documents			
3200_Trusted_Build.doc	HAAT 3200 Controller Trusted Build Guide	1.11	Aug 2010
HAAT_Application_Compilation.doc	HAAT Application Compilation	1.8	Jul 2010
HAAT_DataDictionary.doc	HAAT Data Dictionary	1.02	May 2010
HAAT_OS_Creation.doc	HAAT (Hybrid Activator, Accumulator, & Transmitter) Operating System Trusted Build Guide	1.21	Jul 2010
ICR_Trusted_Build.doc	ICR Trusted Build Guide	1.07	Jun 2010
HAAT100 Documents			
HAAT100_CMPlan.doc	HAAT100 Configuration Management Plan	1.08	Jun 2010
HAAT100_AcceptTest.doc	HAAT100 Acceptance Testing Guide	1.04	Jun 2010
HAAT100_FunctSpec.doc	HAAT100 Functional Specification	1.07	Jun 2010
HAAT100_HardSpec.doc	HAAT100 Hardware Specification HW Revision A0.7 and A.1.2	1.07	Jul 2010
HAAT100_OpMaint.doc	HAAT100 Operations And Maintenance Manual	1.19	Aug 2010
HAAT100_PersTraining.doc	HAAT100 Personnel & Training Requirements	1.04	Jun 2010
HAAT100_PollWorker.doc	HAAT100 Poll Workers Manual	2.09	Aug 2010
HAAT100_QAProgram.doc	HAAT 100 Quality Assurance Program	1.04	Jun 2010
HAAT100_SecSpec.doc	HAAT 100 Security Specification	1.13	Jul 2010
HAAT100_SoftSpec.doc	HAAT 100 Software Specification	1.06	Jun 2010
HAAT100_SysOverview.doc	HAAT 100 System Overview	1.08	Jun 2010
HAAT100_TestVerifSpec.doc	HAAT 100 Test & Verification Specification	1.04	Jun 2010
HAAT100_APL_A07.doc	HAAT 100 Approved Parts List HW Revision A0.7	1.04	Jul 2010
HAAT90 Documents			
HAAT90_AcceptTest.doc	HAAT90 Acceptance Testing Guide	1.08	Jun 2010
HAAT90_CMPlan.doc	HAAT90 Configuration Management Plan	2.08	Jun 2010
HAAT90_FunctSpec.doc	HAAT90 Functional Specification	2.07	Jun 2010
HAAT90_OpMaint.doc	HAAT90 Operations & Maintenance Manual	2.18	Aug 2010
HAAT90_PersTraining.doc	HAAT90 Personnel & Training Requirements	2.04	Jun 2010
HAAT90_QAProgram.doc	HAAT90 Quality Assurance Program	2.05	Jun 2010
HAAT90_SecSpec.doc	HAAT90 Security Specification	2.14	Jul 2010
HAAT90_SysOverview.doc	HAAT90 System Overview	2.10	Jun 2010
HAAT90_TestVerifSpec.doc	HAAT90 Test & Verification Specification	2.04	Jun 2010
HAAT90_PollWorker.doc	HAAT90 Poll Workers Manual	1.11	Aug 2010
HAAT90_SoftSpec.doc	HAAT90 Software Specification	1.08	Jun 2010
HAAT90_APL_A11.doc	HAAT90 Approved Parts List HW Revision A1.1	1.03	Jun 2010
HAAT90_HardSpec.doc	HAAT90 Hardware Specification	1.12	Jul 2010

File Name	Document Title	Revision	Doc Date
HAAT80 Documents			
HAAT80_AcceptTest.doc	HAAT 80 Acceptance Testing Guide	1.04	Jun 2010
HAAT80_APL_A11.doc	Approved Parts List HW Revision A1.1	1.03	Jun 2010
HAAT80_CMPlan.doc	HAAT80 Configuration Management Plan	2.07	Jun 2010
HAAT80_FunctSpec.doc	HAAT80 Functional Specification	2.08	Jun 2010
HAAT80_HardSpec.doc	HAAT80 Hardware Specification	2.07	Jul 2010
HAAT80_OpMaint.doc	HAAT80 Operations & Maintenance Manual	2.17	Aug 2010
HAAT80_PersTraining.doc	HAAT80 Personnel & Training Requirements	2.03	Jun 2010
HAAT80_PollWorker.doc	HAAT80 Poll Workers Manual	1.06	Aug 2010
HAAT80_QAProgram.doc	HAAT80 Quality Assurance Program	2.05	Jun 2010
HAAT80_SecSpec.doc	HAAT80 Security Specification	2.11	Jul 2010
HAAT80_SoftSpec.doc	HAAT80 Software Specification	2.04	Jun 2010
HAAT80_SysOverview.doc	HAAT80 System Overview	2.07	Jun 2010
HAAT80_TestVerifSpec.doc	HAAT80 Test & Verification Specification	2.04	Jun 2010
HAAT50 Documents			
HAAT50_AcceptTest.doc	HAAT50 Acceptance Testing Guide	1.04	Jun 2010
HAAT50_APL_A03.doc	HAAT50 Approved Parts List HW Revision A0.3	1.03	Jun 2010
HAAT50_APL_A11.doc	HAAT50 Approved Parts List HW Revision A1.1	1.03	Jun 2010
HAAT50_CMPlan.doc	HAAT50 Configuration Management Plan	1.07	Jun 2010
HAAT50_FunctSpec.doc	HAAT50 Functional Specification	1.08	Jun 2010
HAAT50_HardSpec.doc	HAAT50 Hardware Specification	1.07	Jul 2010
HAAT50_OpMaint.doc	HAAT50 Operations & Maintenance Manual	1.13	Aug 2010
HAAT50_PersTraining.doc	HAAT50 Personnel & Training Requirements	1.03	Jun 2010
HAAT50_PollWorker.doc	HAAT50 Poll Workers Manual	1.05	Jun 2010
HAAT50_QAProgram.doc	HAAT50 Quality Assurance Program	1.04	Jun 2010
HAAT50_SecSpec.doc	HAAT50 Security Specification	1.09	Jul 2010
HAAT50_SoftSpec.doc	HAAT50 Software Specification	1.04	Jun 2010
HAAT50_SysOverview.doc	HAAT50 System Overview	1.06	Jun 2010
HAAT50_TestVerifSpec.doc	HAAT50 Test & Verification Specification	1.03	Jun 2010
HAAT Listener Build Documents			
SuSE_RAS_Installation.doc	Remote Access Server for HAAT90 Installation Process	1.8	Jul 2010
Source_Code_Compilation_Process.doc	WinEDS/HAAT Listener Source Code Compilation Process (Fast Generation)	1.09	Jun 2010
SuSE_HAATListener_Installation.doc	WinEDS/HAAT Listener Installation Guide	1.16	Jun 2010
HAAT Listener Documents			
Listener_SysOverview.doc	WinEDS/HAAT Listener™ System Overview	1.15	Jul 2010
Listener_CMPlan.doc	WinEDS/HAAT Listener™ Configuration Management Plan	1.13	Jun 2010
Listener_FuncSpec.doc	WinEDS/HAAT Listener™ Functional Specification	1.05	Jun 2010
Listener_OpMan.doc	WinEDS/HAAT Listener™ Operator's Manual	1.12	Jul 2010
Listener_PerTrain.doc	WinEDS/HAAT Listener™ Personnel and Training Requirements	1.03	Jun 2010
Listener_SecSpec.doc	WinEDS/HAAT Listener™ Security Specification	1.13	Jun 2010
Listener_SoftSpec.doc	WinEDS/HAAT Listener™ Software Specification	1.10	Jun 2010
Listener_TDP.doc	WinEDS/HAAT Listener™ Technical Data Package	1.06	Jun 2010
Listener_TestVerifSpec.doc	WinEDS/HAAT Listener™ Test and Verification Specification	1.04	Jun 2010
FEC_X-Ref.doc	FVSS 2002 Vendor Testing and TDP Trace	1.06	Jun 2010
Memory Pack Receiver Documents			
MPR-Penetration.doc	MemoryPack Receiver® Penetration Analysis	1.03	May 2009
MPR_CMPlan.doc	MemoryPack Receiver® Configuration Management	1.06	Jun 2010

File Name	Document Title	Revision	Doc Date
	Plan		
MPR_FEC-Xref.doc	Requirements of the FECVSS 2002 Trace to Vendor Testing and Technical Data Package	1.07	Jun 2010
MPR_FunctSpec.doc	MemoryPack Receiver® Functional Specification	1.04	Jun 2010
MPR_HardSpec.doc	MemoryPack Receiver® Hardware Specification	1.5	Jun 2010
MPR_MaintMan.doc	MemoryPack Receiver® Maintenance Manual	1.8	Jun 2010
MPR_OpMan.doc	MemoryPack Receiver® Operators Manual	1.8	Jun 2010
MPR_PersTraining.doc	MemoryPack Receiver for Optech Insight and Eagle Personnel and Training Requirements	1.05	Jun 2010
MPR_QAProgram.doc	MemoryPack Receiver® Quality Assurance Program	1.04	Jun 2010
MPR_Security.doc	MemoryPack Receiver for Optech Insight/Eagle Security Specification	1.05	Jun 2010
MPR_SoftSpec.doc	MemoryPack Receiver® Software Specification	1.04	Jun 2010
MPR_SysOverview.doc	MemoryPack Receiver® System Overview	1.05	Jun 2010
MPR_TDP.doc	MemoryPack Receiver® Technical Data Package	1.04	Jun 2010
MPR_TestVerifSpec.doc	MemoryPack Receiver® Test and Verification Specification	1.5	Jun 2010
MPR_Security.pdf	MemoryPack Receiver for Optech Insight/Eagle security Specification	1.05	Aug 2010
MPR_APL.doc	MemoryPack Receiver® Approved Parts List	1.02	Jun 2010
MPR_ChgRelSummary.doc	MemoryPack Receiver® Change Release Summary	1.01	Jun 2010
Optech 400-C Documents			
400-C-Penetration.doc	Optech 400-C® Penetration Analysis	1.08	Nov 2009
400-C_ChgRelSummary.doc	Optech 400-C Change Release Summary	1.14	Jul 2010
400-C_CMPlan.doc	Optech 400-C® Configuration Management Plan	1.13	Jun 2010
400-C_FEC-XRef.doc	Requirements of the FECVSS 2002 Trace to Vendor Testing and Technical Data Package	1.16	Jun 2010
400-C_FunctSpec.doc	Optech 400-C® Functional Specification	1.12	Jun 2010
400-C_HardSpec.doc	Optech 400-C® Hardware Specification	1.12	Jun 2010
400-C_MaintMan.doc	Optech 400-C® Maintenance Manual	1.15	Aug 2010
400-C_OpMan.doc	Optech 400-C® Operators Manual	1.22	Aug 2010
400-C_PersTraining.doc	Optech 400-C® Personnel & Training Requirements	1.11	Jun 2010
400-C_QAProgram.doc	Optech 400-C® Quality Assurance Program	1.10	Jun 2010
400-C_Security.doc	Optech 400-C® Security Specification	1.12	Jun 2010
400-C_SoftSpec.doc	Optech 400-C® Software Specification	1.14	Jun 2010
400-C_SysOverview.doc	Optech 400-C® System Overview	1.13	Jun 2010
400-C_TDP.doc	Optech 400-C® Technical Data Package	1.12	Jun 2010
400-C_TestVerifSpec.doc	Optech 400-C® Test & Verification Specification	1.14	Aug 2010
WinETP_RefGuide.doc	WinETP® Reference Guide	1.15	Aug 2010
400-C_APL.doc	Optech 400-C® Approved Parts List	1.09	Jun 2010
Optech Insight and Insight Plus Documents			
INSIGHTp-Penetration.doc	Optech Insight Plus Penetration Analysis (Appendix B To Security Spec)	1.03	Feb 2010
INSIGHTp_APL2.xls	Optech Insight Plus Approved Parts List	1.00	Jan 2009
INSIGHTp_ChgRelSummary.doc	Optech Insight Plus® Change Release Summary	1.06	Jun 2010
INSIGHTp_CMPlan.doc	Optech Insight Plus® Configuration Management Plan	1.07	Jun 2010
INSIGHTp_FEC-XRef.doc	Requirements of the FECVSS 2002 Trace to Vendor Testing and Technical Data Package	1.12	Jun 2010
INSIGHTp_FunctSpec.doc	Optech Insight Plus® Functional Specification	1.08	Jun 2010
INSIGHTp_HardSpec.doc	Optech Insight Plus® Hardware Specification	1.08	Jun 2010
INSIGHTp_MaintMan.doc	Optech Insight Plus® Maintenance Manual	1.10	Jun 2010
INSIGHTp_PersTraining.doc	Optech Insight Plus® Personnel & Training Requirements	1.06	Jun 2010

File Name	Document Title	Revision	Doc Date
OptechPrintersManual.doc	Optech Insight/Eagle and Optech 400-C Printers Manual	1.10	Jun 2010
INSIGHTp_QAProgram.doc	Optech Insight Plus® Quality Assurance Program	1.07	Jun 2010
INSIGHTp_SampleReports.doc	Optech Insight Plus® Sample Reports	1.06	Jun 2010
INSIGHTp_Security.doc	Optech Insight Plus® Security Specification	1.06	Jun 2010
INSIGHTp_SoftSpec.doc	Optech Insight Plus® Software Specification	1.08	Jun 2010
INSIGHTp_SysOverview.doc	Optech Insight Plus System Overview	1.08	Jun 2010
INSIGHTp_TDP.doc	Optech Insight Plus® Technical Data Package	1.09	Jun 2010
INSIGHTp_TestVerifSpec.doc	Optech Insight Plus® Test & Verification Specification	1.07	Jun 2010
InsightBattery_PollWorkerOp.doc	Insight Battery® Poll Workers & Operators Manual	1.04	Jun 2010
INSIGHT-INSIGHTplus_OpMan.doc	Optech Insight/Insight Plus Operators Manual	1.16	Aug 2010
INSIGHTp_APL.doc	Optech Insight Plus® Approved Parts List	1.06	Jun 2010
WinEDS Documents			
WinEDS4-0_PersTraining.doc	WinEDS Personnel & Training Requirements Release 4.0	1.05	Jun 2010
Software_Quality_Assurance_Program.doc	Software Quality Assurance Program Release 4.0	1.06	Jun 2010
WinEDS4-0_SampleReports.doc	WinEDS Sample Reports Release 4.0	1.07	Jun 2010
WinEDS4-0_SysDatabase.doc	WinEDS System Database Release 4.0	1.11	Jun 2010
WinEDS4-0_VisioTemplates-EDGE.doc	WinEDS Visio Templates: Edge/EDGE2plus Release 4.0	1.05	Jun 2010
WinEDS 4-0_TestVerifSpec.doc	WinEDS Test & Verification Specification Release 4.0	1.07	Jun 2010
WinEDS4-0_FunctSpec.doc	WinEDS Functional Specification Release 4.0	1.05	Jun 2010
WinEDS4-0_GUI.doc	WinEDS Graphical User Interface Release 4.0	1.05	Aug 2010
WinEDS4-0_Security.doc	WinEDS Security Specification Release 4.0	1.15	Aug 2010
WinEDS4-0_TDP-XRef.doc	SVS WinEDS 4.0 – TDP Cross-Reference	1.08	Jun 2010
WinEDS4-0Sys_Ops_Proc.doc	WinEDS System Operations Procedures Release 4.0	1.30	Aug 2010
WinEDS_4-0_Build_Process_LOCAL.doc	WinEDS Local Build Process Release 4.0	1.16	Aug 2010
WinEDS4-0_CM_ Plan.doc	WinEDS Configuration Management Plan Release 4.0	1.06	Jun 2010
WinEDS4-0_TDP.doc	WinEDS Technical Data Package Release 4.0	1.05	Jun 2010
WinEDS4-0ExtSvcs_OpMan.pdf	WinEDS Extended Services Operator's Guide Release 4.0	2.20	Aug 2010
WinEDS_4-0_Software_Spec.pdf	WinEDS Software Specification Release 4.0	1.19	Aug 2010
WinEDS4_0_Master_Doc_Chng_Log.doc	WinEDS 4.0 Technical Data Package Master Document Change Log	0.18	Jun 2010
WinEDS4-0_RCV_Func_Spec.pdf	WinEDS Ranked Choice Voting Functional Specification Release 4.0	1.16	Jul 2010
WinEDS4_0_Install_Gd.pdf	WinEDS Installation Guide Release 4.0	1.14	Jun 2010
WinEDS4-0_System_Overview.pdf	WinEDS System Overview Release 4.0	1.11	Jul 2010
WinEDS4-0_ElecRptg_OpMan.pdf	WinEDS Election Reporting Operator's Guide Release 4.0	2.17	Aug 2010

Table 11 Other Software, Hardware and Materials

Material	Material Description	Use in the Voting System
Multiple desktop and laptop PCs	A variety of PCs running Microsoft operating systems	Supplied by iBeta: Preparation, management and recording of test plans, test cases, reviews and results
Repository servers	Separate servers for storage of test documents and source code, running industry standards operating systems, security and back up utilities	Supplied by iBeta: Documents are maintained on a secure network server. Source code is maintained on a separate data disk on a restricted server
Microsoft Office 2003	Excel and Word software and document templates	Supplied by iBeta: The software used to create and record test plans, test cases,

Material	Material Description	Use In the Voting System
		reviews and results
SharePoint 2003	TDP and test documentation repository	Supplied by iBeta: TDP and test documentation repository and configuration management tool
Other standard business application software	Internet browsers, PDF viewers email	Supplied by iBeta: Industry standard tools to support testing, business and project implementation
Center 325 Mini Sound Level Meter	IEC 651 Type 2 handheld sound level meter	Supplied by iBeta: Measure decibel level
Wagner Instruments Force Gage	Model FDN 50	Supplied by iBeta: Gage to measure force
Visual Studio 2003 v.7.1.3808 (Microsoft)	Build and source code review Integrated Development Environment	Supplied by iBeta: View source code review
RSM v.6.92 (M Squared Technologies)	C, C++, Java & C# static analysis tool	Supplied by iBeta: Identify line counts and cyclomatic complexity
Beyond Compare 2 v.2.4.3 (Scooter Software)	Comparison utility	Supplied by iBeta: Used to compare file/folder differences
WinDiff 5.1 (Microsoft)	Comparison utility	Supplied by iBeta: Used to compare file/folder differences
Hash.exe v.7.08.10.07.12 (Maresware)	Hash creation utility	Supplied by iBeta: Used to generate hash signatures for Trusted Builds
Nessus v.4.0.0	Network port scanner and vulnerability testing tool	Supplied by iBeta: Used to scan ports of Public Telecommunications Networking for vulnerabilities v3.2.0 prior to 10/16/2009 and then v4.0.0. Plug-in Rev 200910052134
WireShark v. 1.0 (Formerly Ethereal v. 0.99.0)	An open source network packet capture and analysis tool	Supplied by iBeta: Used to capture packets for later analysis of cryptography
MiniMaxwell v2.0/10	Network emulation and impairment tool	Supplied by iBeta: used to emulate network impairments for telephony test cases.
BartPE ghost32.exe (916 CD)	OS to boot to for ghosting	Disk image backups for testing repeatability.
Norton Symantec Ghost v.11	Tool to create and restore ghost images	Disk image backups for testing repeatability and for Trusted Build submission to the NSRL

4 Voting System Overview

The Sequoia 4.0 Voting System consists of the following hardware and software:

- **WinEDS 4.0** is a client/server election management application for programming and tabulating election results. The election is defined and then applied to the voting machine(s), providing the machine with the logic needed to tabulate the results entered by the voter on the machine. Supports single input of customer profile data such as voting locations, precincts, political subdivisions, offices, parties and machines and uses this data to simultaneously manage multiple elections by multiple users. In addition, the system supports the use of multiple voting systems within any given election. WinEDS has two add-in applications:
  - **Election Reporting** module enables you to run reports and export data.
  - **Extended Services** has several different modules at this time:
    - **Data Manager**
    - **Manual Data Entry**
    - **Media Loader**
    - **Ranked Choice Voting**
    - **Selection Code Generator**

- **WinEDS/HAAT Listener** is a server-based application designed to receive encrypted unofficial electoral data and, optionally, configuration data and event logs, from previously authorized transmitting HAAT devices. The WinEDS/HAAT Listener validates the integrity of all data received, and stores it in a centralized database management system (DBMS).

  HAAT devices can also use the WinEDS/HAAT Listener server to synchronize their time and date with that of the server, so all HAAT devices will have an approximately similar time. The application is designed to run on a redundant server network with as many interconnected servers so as to be able to handle all concurrent transmissions from multiple external devices. The HAAT Listener runs on an application server; uses a web server to connect and receive electoral data from transmitting devices; and temporarily queues the data to an internal database before validating and sending it to the DBMS.

  The HAAT Listener System Components include:
  - Application Server
  - Listener application
  - Local Database
  - Central Database

- **AVC Edge II** is a DRE voting system that displays ballot content to a voter utilizing touch screen technology, electronically stores vote totals and audit trail voting activity and provides a method to transfer totals to a central tabulation center.
  - **VeriVote Printer (Voter Verifiable Paper Audit Trail)** is side-mounted onto an AVC Edge II to produce a paper record of the voter's selections for review. Various reports can be printed, and once polls are closed, a report is generated with the results for each candidate.
  - **AVC Edge II Audio Voting Accessory (E-AVA)** provides independent voting capability for visually impaired or other non-reading voters utilizing a keypad and audio scripts.
  - **Card Activator** serves as the voter's access to the AVC Edge II through a Smart Card activation interface.
  - **Seiko DPU-414 printer** is an optional 40 column thermal dot matrix printer by Seiko, used to provide election reports.
  - **Edge Aux Power Unit** is an Auxiliary Backup Power Unit that provides emergency power for two AVC Edge machines for an extended period of time.

- **EDGE2*plus*** Model 300 (HW Rev. C.03 & C.04) and Model 305 (HW Rev. C.04) are designed as DRE voting systems that displays ballot content to a voter utilizing touchscreen technology, electronically stores vote totals and audit trail voting activity and provides a method to transfer

totals to a central tabulation center. The Model 300 includes the ABLE-D detachable audio voting control, model 305 does not.

- **Audio Voting Control (ABLE-D)** is a simple eight-button device designed for use with the EDGE2*plus* Model 300. The ABLE-D provides unassisted, private and secure voting for voters with serious limitations to using their hands, as well as visually impaired and non-reading voters.
- **APS External Printer (UTG)** is a Voter Verifiable Paper Audit Trail printer (not part of the certification test campaign) that is side mounted onto an EDGE2*plus* to produce a paper record of the voter's selections for review.
  Various reports can be printed, and once polls are closed, a report is generated with the results for each candidate.

- **Hybrid Activator, Accumulator, and Transmitter (HAAT)** enables the voter to access the AVC Edge II and EDGE2*plus* voting machines through a smart card interface. Some versions of the HAAT have additional functionality.
  - **HAAT100** The unit also serves at the precinct level as an accumulator for consolidating and tallying results, a printer for printing results, and as a transmitter for transmitting results from the AVC Edge II, EDGE2*plus*, and Insight voting machines only.
  - **HAAT90** The unit also serves at the precinct level as an accumulator for consolidating and tallying results, a printer for printing results, and as a transmitter for transmitting results from the AVC Edge II, EDGE2*plus*, and Insight voting machines only.
  - **HAAT80** The unit also serves at the precinct level as an accumulator for consolidating and tallying results, and a printer for printing results from the AVC Edge II, EDGE2*plus*, and Insight voting machines only.
  - **HAAT50** Only serves as voter's access to the AVC Edge II and EDGE2*plus* voting machines through activation of a smart card interface.
  - **Insight Memory Pack Reader (iMPR)** allows the HAAT80/90/100 to read and consolidate Insight data cartridges. This device must be connected to the HAAT80/90/100 serial port located at the back of the unit.

- **Optech Insight & Optech Insight Plus** are portable Precinct Count Systems that sit atop a ballot box, that uses Optical Scan Read-Head technology to electronically read and tabulate Optical Scan ballots, store results, and print precinct totals at the Polling Place.
  - **Memory Pack** is a solid-state semiconductor portable cartridge whose software records and totals all of the information from the ballots inserted into an Optech Insight and Optech Insight Plus. The MemoryPack is equipped with customized chips, which each has a specific function.
  - **Memory Pack Receiver (MPR)** is a desktop device, which is plugged into a computer to interface with WinEDS 4.0 to write election parameters to MemoryPacks, as well as read and tally election results from those same MemoryPacks.

- **Optech 400-C Central Count System** is a standalone, self-contained optical scan ballot tabulator that uses an automatic ballot feeder to process ballots. The Optech 400-C can process about 400 ballots per minute depending upon the ballot length. It also simultaneously reads the front and back of each ballot card.
  - **WinETP Election Tabulation Program** is an election tabulation application that enables the Optech 400-C to tabulate ballots and report results. WinETP interfaces with WinEDS to receive the election definition and process 400-C Results.

The following table identifies the maximum evaluated and calculated limits for WinEDS and the associated Sequoia machines.

Table 12 WinEDS 4.0 System Limits

Characteristic	Evaluation Limit	Calculated Limit	Limiting Component	WinEDS	Insight	400C	Edge
Maximum precincts in election	2,700	5,000	400C	10,000,000	NA	5,000	NA
Maximum precincts in a pack	150	200	Insight	NA	200*	NA	9999

Maximum contests in election	2,019	5,000	400C	10,000,000	NA	5,000	NA
Maximum candidates/ counters in election	6,532	8,000	400C	10,000,000	NA	8,000	65,535
Maximum candidate counters in a precinct	350	1,023	Insight	10,000,000	1,023	8,000	65,535
Maximum ballot styles in election	2,520	10,000	400C	2,000,000,000	NA	10,000	NA
Maximum contests in a ballot style	110	700	Insight/400C	10,000,000	700	700	65,535
Maximum candidates in a contest	348	700	Insight/400C	10,000,000	700	700	65,535
Maximum ballot styles in a Precinct	100	100	Insight	2,000,000,000	100	1,024	1,024
Maximum number of parties	15	15	Insight/400C	36	15	15	255
Maximum vote for in contest	150	255	Edge	10,000	1,023	1,023	255

* For the Insight, the maximum number of precincts that fit on a cartridge is dependent on the complexity of the election. The limit of 200 is based on a single candidate/single contest ballot.

4.1 *Election Management System- Pre Voting Capabilities*

4.1.1 WinEDS 4.0

WinEDS is a client/server election management application for programming and tabulating election results. Vote tabulation equipment currently supported by WinEDS 4.0 includes:

- AVC Edge II
- AVC EDGE2*plus*
- Optech 400-C
- Optech Insight Plus
- Optech Insight

The system has been designed to support single input of customer profile data such as voting locations, precincts, political subdivisions, offices, parties and machines and use this data to simultaneously manage multiple elections by multiple users. In addition, the system supports the use of multiple voting systems within any given election.

WinEDS 4.0 has two add-in applications:

- WinEDS Extended Services
- WinEDS Election Reporting

The Election Reporting module enables you to run reports and export data. Extended Services has several different modules at this time, Data Manager, Manual Data Entry, Media Loader, Ranked Choice Voting, and Selection Code Generator.

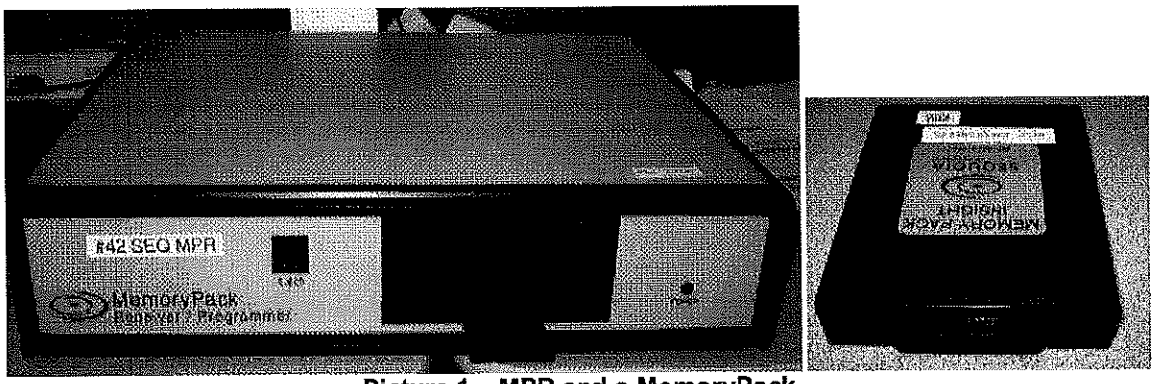
4.1.2 Memory Pack Receiver (MPR) for the Optech Insight/InsightPlus

The MPR is an interface that allows WinEDS 4.0 to write election parameters to MemoryPacks, as well as read and tally election results from those same MemoryPacks.

The MPR is a desktop device, which is plugged into a computer (usually at the election central site), and developed specifically to work in conjunction with WinEDS 4.0 (Windows Election Database System) to encode precinct election data from WinEDS 4.0 to a MemoryPack.

The MemoryPack is then placed in the Optech Insight for that precinct and ballots are tabulated by the MemoryPack.

After the election, the MemoryPacks from each precinct are inserted back into the MPR. The ballot tabulation totals stored in each MemoryPack are read by WinEDS 4.0 software, which accumulate the jurisdiction-wide results.



Picture 1 – MPR and a MemoryPack

4.2 *Polling Place- Voting Capabilities*

The AVC Edge II and AVC EDGE2*plus* do not require any networking to a central system in order to function. All processing from loading the ballot to recording votes is done on individual units. Loading ballots and accumulating the tally from the machines is completed via the Results Cartridge. The Results Cartridge is designed so that it can be inserted into the voting machine, record voting results, and then be removed from the machine when the polls are closed to be read by WinEDS.

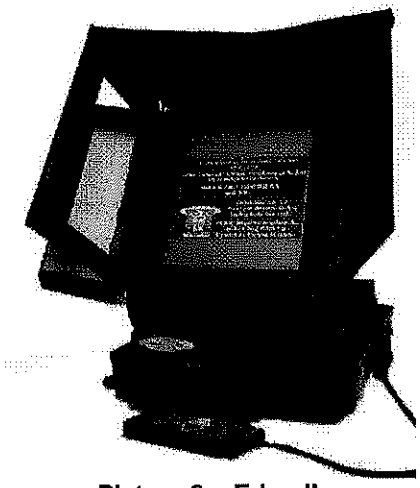
The Results Cartridge stores:

- An electronic representation of the ballot
- Ballot logic to enable the voter to make those selections to which he or she is lawfully entitled
- Aggregated vote totals
- A randomized record of all individual ballots cast
- A chronological log of significant machine operations, including error conditions

4.2.1 AVC Edge II

The AVC Edge II is designed as a DRE voting system that performs the following functions:

- Present candidates and issues using an electronic ballot.
- Display a series of buttons/switches/images to be touched/pressed for selecting a candidate or option. Indicators display to the voter or operator their selections.
- Prevent overvoting of offices.
- Allow the voter to select and deselect a candidate position right up until the Cast Ballot button is touched.
- Allow for electronic Write-In voting.
- Operate on AC to DC External Power Supply and incorporate Main and Real-Time Clock batteries for backup protection.
- Provide for voting privacy.
- Electronically store vote totals and a complete Audit Trail of voting activity.
- Print results for each candidate when the polls are closed.
- Provide a method to transfer machine totals to a central tabulation center.
- Have tamper resistant design using locks, seals and cryptography to provide security.



Picture 2 – Edge II

The AVC Edge II includes the following accessories:

- **Card Activator**
  The Card Activator serves as the voter's access to the AVC Edge II machines through a Smart Card activation interface. The Poll Worker issues this card to the voter for use as a key to access the ballot on the AVC Edge II, for voting purposes.

Picture 3 – Card Activator

- **VeriVote Printer**
  The VeriVote Printer produces a paper record that can be reviewed by the voter as they cast their vote.
  Designed
  • As an upgrade to existing units installed at jurisdictions across the county or country,
  • As an optional feature with a new AVC Edge II.

  The VeriVote Printer is designed to be shipped as a separate item from the AVC Edge II and installed in the polling place/precinct by Precinct/Poll Workers.

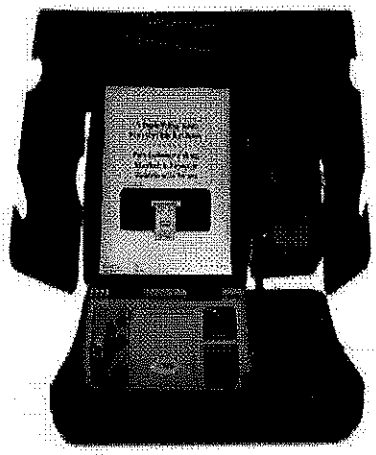
- **AVC Edge II Audio Voting Accessory**
  Provides independent voting capability for visually impaired or other non-reading voters by utilizing a keypad and audio scripts.

  With the proper ballot configuration, any AVC Edge II can be used with the AVC Edge II Audio Voting Accessory on demand.

4.2.2 EDGE2*plus*

The EDGE2*plus* Models 305 and 300 are designed as DRE voting systems. The Model 300 includes the ABLE-D detachable audio voting control. Both models will perform the following functions:

- Present candidates and issues by using an electronic ballot.
- Display a series of buttons/switches/images to be touched/pressed for selecting a candidate or option. Indicators show the voter or operator that the selection has been made.
- Prevent overvoting of offices.
- Allow the voter to select and deselect a candidate position right up until the Cast Ballot button is touched.
- Allow for electronic Write-In voting.
- Operate on AC to DC External Power Supply and incorporate Main and Real-Time Clock batteries for backup protection.
- Provide for voting privacy.
- Electronically store vote totals and a complete Audit Trail of voting activity.
- Print results for each candidate when the polls are closed. (Not Certified)
- Provide a method to transfer machine totals to a central tabulation center.
- Have tamper resistant design using locks, seals and cryptography to provide security.
- The Detachable Audio Voting Control (ABLE-D) is a simple eight-button device designed for use with the EDGE2*plus* Model 300 voting system. The ABLE-D allows unassisted, private and secure voting for voters with serious limitations to using their hands, as well as visually impaired and non-reading voters.



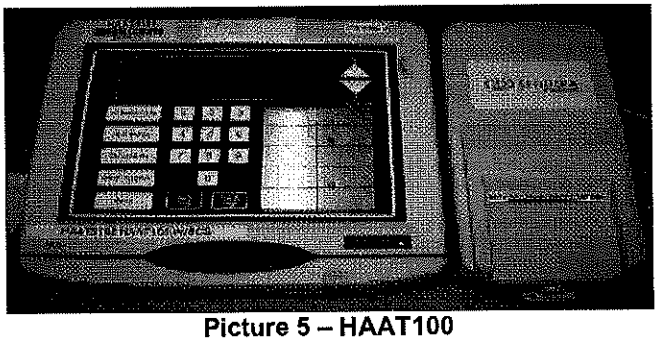
Picture 4 – EDGE2*plus*

4.2.3 HAAT

The Hybrid Activator, Accumulator, and Transmitter (HAAT) enables the voter to access the AVC Edge II, EDGE2*plus*, and Insight voting machines through a smart card interface. Some versions of the HAAT have additional functionality.

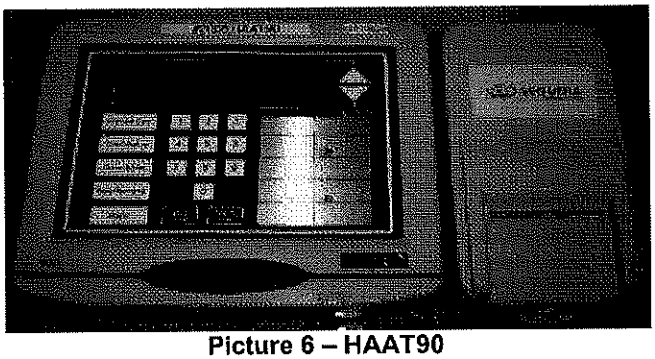
HAAT100

The HAAT100 is the component that serves as the voter's access to the AVC Edge II, EDGE2*plus* direct-record electronic touch-screen voting machines through activation of a Smart Card interface. The HAAT100 Unit also serves, at the precinct level, as an accumulator for consolidating and tallying results, a printer for printing the results, and as a transmitter for transmitting the results from the AVC Edge II, EDGE2*plus*, and Insight voting machines only.



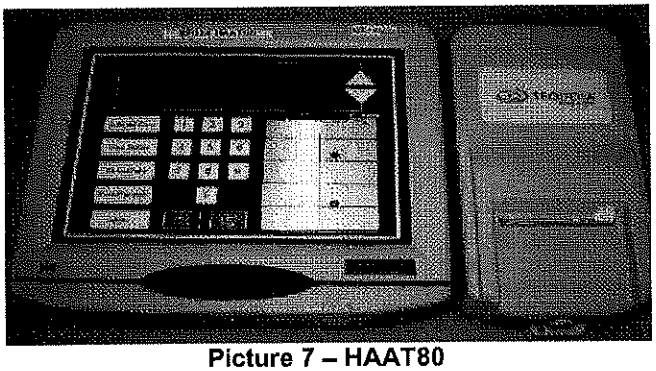
Picture 5 – HAAT100

HAAT90
The HAAT90 is the component that serves as the voter's access to AVC Edge II and EDGE2*plus* DRE touch-screen voting machines through activation of a Smart Card interface. The HAAT90 Unit also serves, at the precinct level as an accumulator for consolidating and tallying results, a printer for printing the results, and as a transmitter for transmitting the results from the AVC Edge II, EDGE2*plus*, and Insight voting machines only.



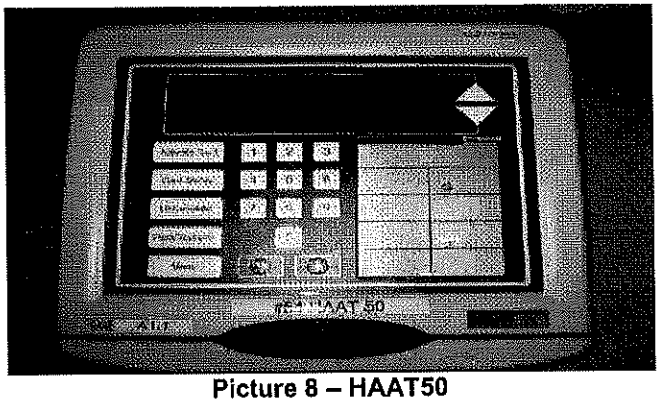
Picture 6 – HAAT90

HAAT80
The HAAT80 is the component that serves as the voter's access to AVC Edge II and EDGE2*plus* direct-record electronic touch-screen voting machines through activation of a Smart Card interface. The HAAT80 Unit also serves, at the precinct level, as an accumulator for consolidating and tallying results, and a printer for printing the results from AVC Edge II, EDGE2*plus*, and Insight voting machines only.



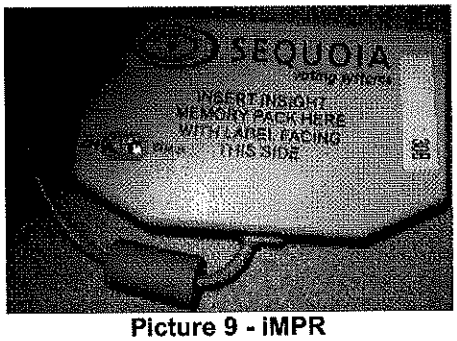
Picture 7 – HAAT80

HAAT50
The HAAT50 is the component that serves as the voter's access to AVC Edge II and EDGE2*plus* direct-record electronic touch-screen voting machines through activation of a Smart Card interface.
Note: The HAAT50 does not consolidate, print or transmit results, since the HAAT50 does not use any printer or internal modem and the consolidation module is not available.



Picture 8 – HAAT50

Insight Memory Pack Reader for use with the HAAT80/90/100
The Insight Memory Pack Reader (iMPR) allows the HAAT80/90/100 to read and consolidate Insight data cartridges. This device must be connected to the HAAT80/90/100 serial port located at the back of the unit.



Picture 9 - iMPR

4.2.4 Optech Insight Plus

The Optech Insight and Optech Insight Plus are portable Precinct Count Systems, which use Optical Scan Read Head technology to electronically read and tabulate Optical Scan ballots. The machines are designed as Precinct Count systems that will work in conjunction with WinEDS, as follows:

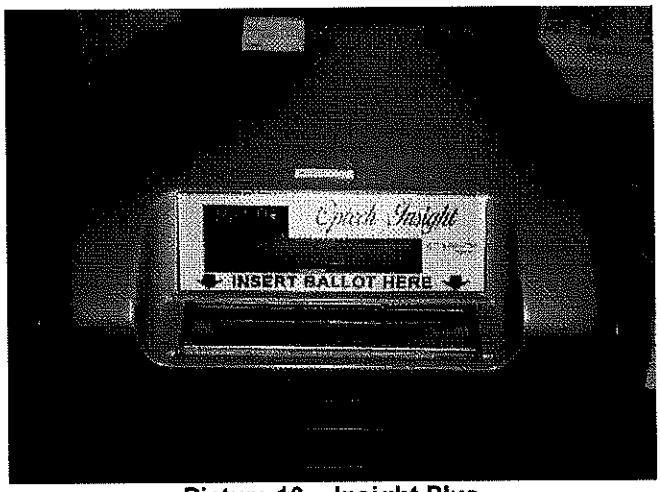
- To code the election and prepare the Ballot.
- To accumulate, translate, and generate reports at the Central Counting Location

The machines are intended to be located at the Polling Place. The voter casts a vote on the ballot by using a special Optech marking pen (or a soft lead #2 pencil) to complete a printed voting arrow pointing to the candidate/issue of the voter's choice. The voter then places the marked ballot into the system in any orientation. The machine keeps a running tabulation on all ballots "cast." The Optech Insight and Optech Insight Plus use the Election Parameter data programmed into the MemoryPack using WinEDS. The MemoryPack may be removed at the end of the election and transported to the Central Counting Location for rapid transfer of precinct totals to the Central Counting Location for inclusion into the canvass reports. After the election, the MemoryPacks from each precinct are inserted back into the MPR. The ballot tabulation totals stored in each MemoryPack are read by WinEDS software, which accumulates the jurisdiction-wide results.

The Optech Insight Plus is a portable Precinct Count System that uses Optical Scan Read Head technology to electronically read and tabulate Optical Scan ballots at the Polling Place. The Optech Insight Plus is classified by the Federal Election Commission as a Marksense Voting System used to cast and tabulate ballots. It allows Local Officials to conduct efficient, timely elections, and performs the following functions using the voter inserted ballots:

- Record Votes: Optically reads the marks made on the ballots.

- Tabulate Ballot: Tabulates ballots as they are cast, allowing the results of the election to be readily available when closing the Polls.
- Print Results: Produces precinct totals.
- Store Election Totals: Stores the election totals in the removable Memory-Pack, for easy transfer to the Central Counting Location, after closing the Polls.



Picture 10 – Insight Plus

4.2.5 Optech Insight

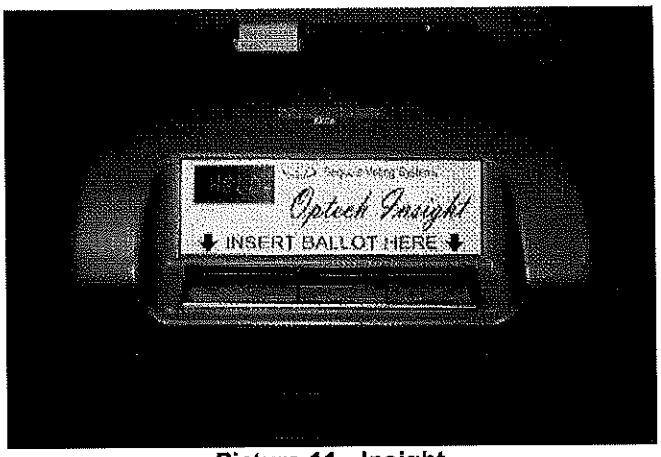
The Optech Insight is a portable Precinct Count System that uses Optical Scan Read-Head technology to electronically read and tabulate Optical Scan ballots at the Polling Place. The Optech Insight is classified by the Federal Election Commission as a Marksense Voting System used to cast and tabulate ballots. It allows Local Officials to conduct efficient, timely elections, and performs the following functions using the voter inserted ballots:

- Record Votes: Optically reads the marks made on the ballots.
- Tabulate Ballot: Tabulates ballots as they are cast, allowing the results of the election to be readily available when closing the Polls.
- Print Results: Produces precinct totals.
- Store Election Totals: Stores the election totals in the removable Memory-Pack, for easy transfer to the Central Counting Location, after closing the Polls.

The MemoryPack is a solid-state semiconductor portable cartridge whose software records and totals all of the information from the ballots inserted into one of the following voting systems:

- Optech Insight
- Optech Insight Plus

The MemoryPack is equipped with customized chips, which each has a specific function. After a MemoryPack is inserted into the Memory Pack Receiver (MPR), the election results can be read into the WinEDS 4.0 software (which is installed on the computer connected to the MPR), and displayed by the computer. The Optech Insight uses the Memory Pack Receiver to apply the election parameters to the tabulator and following the election, to read and tally election results.



Picture 11 - Insight

4.3 *Election Management System- Post Voting Capabilities*

4.3.1 Optech 400-C Central Count System

The WinEDS election definition is applied to the Optech 400-C via the WinETP to enable the 400-C to tabulate ballots and report results. The interface between the WinETP and WinEDS comprises the following:

- Functions
- Events and Properties
- Build Processes

The WinEDS 4.0 database system includes a file management system with the following capabilities:

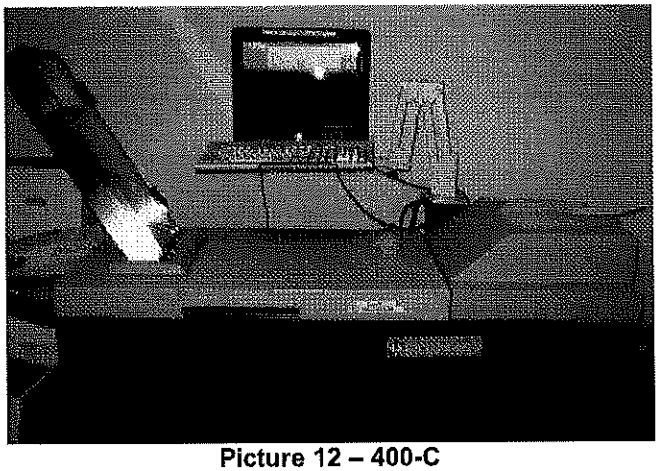
- Integration of Voting Data Files with Ballot Definition Files
- Verification of File Compatibility: File compatibility verification
- Edit and Update of Files: File updating and editing, as required

The Optech 400-C does not provide the Vote Data Management. WinEDS provides the management, processing and reporting of voting data after consolidation at the polling place and includes hardware and software required to generate all output reports in the various jurisdictional required formats at the Central Counting Location.

The Optech 400-C is a standalone, self-contained optical scan ballot tabulator that uses an automatic ballot feeder to process ballots. The Optech 400-C can process about 400 ballots per minute depending upon the ballot length. It also simultaneously reads the front and back of each ballot card. The Optech 400-C is classified by the Federal Election Commission as a Marksense Voting System.

The Optech 400-C is used at the Central Count Location to perform the following activities:

- Open Polls
- Read mark-sense ballots
- Tabulate the results
- Prepare output reports
- Prepare results files for tally and accumulation in WinEDS



Picture 12 – 400-C

4.3.2 WinETP Election Tabulation Program

The WinETP integrates with the Optech 400-C and the WinEDS election management system. The 400-C counts the ballots and applies the results using the logic in the WinETP from the WinEDS system. This interface enables the 400-C to tabulate the election results from large numbers of ballot at a central count location. WinETP is used to perform the following operations:

- Apply and initialize the election
- Tabulate ballots by:
  - Precinct
  - Batch
  - Polling Place
- Manage ballot handling
- Generate reports

WinETP interfaces with WinEDS to receive the election definition and process 400-C Results. The WinEDS system communicates with the WinETP by describing the following for a specific election:

- Offices
- Candidates
- Precincts

WinEDS is a computer software system, which contains the application software developed specifically for election requirements.

4.3.3 Memory Pack Receiver (MPR) for the Optech Insight/Insight Plus

The MPR is an interface that allows WinEDS 4.0 to write election parameters to MemoryPacks, as well as read and tally election results from those same MemoryPacks.

The MPR is a desktop device, which is plugged into a computer (usually at the election central site), and developed specifically to work in conjunction with WinEDS 4.0 (Windows Election Database System) to encode precinct election data from WinEDS 4.0 to a MemoryPack.

The MemoryPack is then placed in the Optech Insight for that precinct and ballots are tabulated by the MemoryPack.

After the election, the MemoryPacks from each precinct are inserted back into the MPR. The ballot tabulation totals stored in each MemoryPack are read by WinEDS 4.0 software, which accumulate the jurisdiction-wide results.

4.3.4 WinEDS/HAAT Listener

WinEDS/HAAT Listener is a server-based application designed to receive encrypted unofficial electoral data and, optionally, configuration data and event logs, from previously authorized transmitting HAAT

devices. The WinEDS/HAAT Listener runs under JBoss version 4.0.2, which is a Java 2 Enterprise Edition (J2EE) compliant Application Server. The Listener Application uses a Web Service to process connections and transmissions from remote clients (HAAT devices) and store encrypted, unofficial results after a series of validations. The WinEDS/HAAT Listener validates the integrity of all data received, and stores it in a centralized database management system (DBMS). HAAT devices can also use the WinEDS/HAAT Listener server to synchronize their time and date with that of the server, so all HAAT devices will have an approximately similar time. Transmissions may include:

- Voting Machine Results
- HAAT Event Log
- HAAT Configuration Data

All data transferred from the HAAT devices to the Listener is:

- Encrypted
- Unofficial
- In XML format
- Validated against an XSD schema
- Validated against a separate transmitted hash string to detect any loss of data
- Stored in a local repository for auditing purposes

WinEDS/HAAT Listener uses a local database to store backups of every correct and incorrect transmission received through the Web service as well as to handle all seven messaging queues used by the core of the Listener application for asynchronous data transfer among objects.

WinEDS/HAAT Listener uses a central database, common for all possible instances of the distributed application to store all voting machine results, HAAT event logs and HAAT configurations received through the Web Service. Additionally, this database holds a tabulated, organized, and centralized copy of all Listener instances event log records.

5 Certification Review and Test Results

The results and evaluations of the PCA and FCA reviews tests are identified below. Detailed data regarding the Acceptance/Rejection criteria, reviews and tests are found in the appendices.

- Appendix A identifies all certification test requirements traced to specific Test Cases
- Appendix B identified the PCA Source Code Review Acceptance/Rejection Criteria and Summary
- Appendix C identifies the PCA TDP Document Review Acceptance/Rejection criteria
- Appendix D identifies all FCA Testing Acceptance/Rejection criteria
- Appendix E identifies the PCA and FCA Discrepancies reported during review and testing

5.1 *PCA Source Code Review*

iBeta Quality Assurance reviewed the Sequoia internally developed coding standards for the software submitted in section 3 in certification of the Sequoia WinEDS 4.0 Voting System. Review criteria were customized to incorporate the requirements of *VSS 2002* Vol. 1 Sect 4.2 and Vol. 2 Section 5, language specific conventions (PowerBuilder, Java, C, C++, C#, VB.net, VB 6, Z80, 80x86, 8051, PIC-ASM, and SQLScript) and the internally developed coding standards as referenced. The specific review criteria for this test effort and the documentation of the building of the executable code from the reviewed source code (Trusted Builds) are identified in Appendix G.

iBeta tracked a number of metrics obtained from the results of the source code review during this certification test campaign. The overall summary of the source code review produced the following metrics as identified in Table 13. The legend of this table is as follows:

- Application - Each WinEDS 4.0 voting system application as defined in Table 9.
- Language - The software coding language. The four Assembler languages (Z80, 80x86, 8051, and PIC-ASM) are reported in one metric.
- Discrepancies - Discrepancies are written against a module which may be defined as either a file or a function within a source code file and, as such, each discrepancy may represent one or more instance of non-compliance with a *VSS 2002* requirement.
- VSS Requirements: Comment Related - The number of comment related instances of non-compliance with 15 *VSS 2002* requirements related to commenting and formatting (considered having a higher impact on software maintainability but a lower impact on system function).
- VSS Requirement: Software Related - The number of software related instances of non-compliance with 29 *VSS 2002* requirements that may impact software function.
- Number of files/functions - Modules are defined for each language and the source code review is conducted at a module or function level. Any code outside of a module or function is reviewed at the file level.
- eLOCs - Number of executable Lines of Code (eLOC). eLOC does not include comment lines, headers, blank lines, spacing, formatting, or continues.
- Metrics: Discrepancy to eLOC - An overall discrepancy-to-eLOC (executable Lines of Code) percentage.
- Metrics: Comment Related % - An overall comment related percentage of the number of instances noted during the source code review.
- Metrics: Software Related % - An overall software related percentage of the number of instances noted during the source code review.

Analysis and summary of the source code review results delineated by coding language is provided in the following sections.

Table 13 Source Code Review Applications and Summary Metrics

Application	Language	Discrepancies	*VSS 2002* Requirements		Number of files/ functions	eLOCs	Metrics		
			Comment Related	Software Related			Discrepancy to eLOC %	Comment Related %	Software Related %
WinEDS	PowerBuilder	1648	1755	116	9058	191126	0.86%	94%	6%
WinEDS	C/C++	2961	2727	1188	11321	216173	1.37%	70%	30%
Card Activator									
Edge II Audio Unit									
Edge II Firmware									
CRC Util									
iMPR									
WinETP (400-C)									
EDGE2*plus*									
HAAT									
HAAT									
WinEDS	SQL	620	193	575	1320	99334	0.62%	25%	75%
WinEDS									
WinEDS	C#	2882	2702	1017	11606	120307	2.40%	73%	27%
EDGE2*plus*									
HAAT									
WinEDS	VB 6.0	196	227	97	324	9094	2.16%	70%	30%
WinEDS	VB.Net	429	359	289	1206	17376	2.47%	55%	45%
HAAT Listener	Java	152	125	75	476	3578	4.25%	63%	38%
HAAT									
HAAT									
Edge II Firmware	Assembler	258	63	229	1219	25776	1.00%	22%	78%
EDGE2*plus*									
Insight/Insight Plus APX									
Insight/Insight Plus HPX									
HAAT									
VeriVote									
MPR									
Total		9146	8151	3586	35275	682764	1.34%	69%	31%

5.1.1 WinEDS 4.0 PowerBuilder Source Code Review Results

WinEDS 4.0 consists of a PowerBuilder (or PowerScript) component. A total of 9058 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 1648 discrepancies were identified and validated to be resolved. Those 1648 discrepancies encompassed 1871 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (1755) of those instances were comment related. Of the software related instances (the remaining 116), the summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified no files or functions that exceeded 240 eLOCs.

v.1: 4.2.3.d v.2: 5.4.2.1	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS	**Version 4.0.158**	PowerScript 10.5	7195	500	112	0	7807
			92.16%	6.40%	1.43%	0.00%	100.00%

Comment Related Instances/Discrepancies
Of the total 1871 *VSS 2002* requirement non-compliances, 1755 or 94% were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, lines exceeding 80 characters, incomplete header information, and non-unique module use.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 116 non-compliances or 6% of identified issues. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002.* The data supporting this review are found in Appendix B.

5.1.2 WinEDS 4.0 C/C++ Source Code Review Results

WinEDS 4.0 consists of numerous C and C++ components. A total of 11,321 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 2961 discrepancies were identified and validated to be resolved. Those 2961 discrepancies encompassed 3915 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (2727) of those instances were comment related. The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The SQL files function line count results identified 4 files or functions that exceeded 240 eLOCs with the justification provided that these files/functions were not placed into separate functions for performance.

v.1: 4.2.3.d v.2: 5.4.2.I	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS		C/C++	10290	767	212	4	11273
			91.3%	6.8%	1.9%	0.04%	100.00%

Comment Related Instances/Discrepancies
Of the total 3915 *VSS 2002* requirement non-compliances, 2727 or 69.7% were rejected against the 14 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, functions with more than 5 levels of indented scope, lines exceeding 80 characters, constants other than "0" or "1" not defined, incomplete header information, and non-unique module use.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 1188 non-compliances or 30.3% of identified issues. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002*. The data supporting this review are found in Appendix B.

5.1.3 WinEDS 4.0 SQL Source Code Review Results

WinEDS 4.0 consists of an SQL component. A total of 1320 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 620 discrepancies were identified and validated to be resolved. Those 620 discrepancies encompassed 768 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (575) of those instances were related to transaction updates within the database. The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified 20 files/ functions that exceeded 240 eLOCs and that more than 5% exceeded 120 eLOCs all with the justification provided that these files/functions contained only database setup commands and had a cyclomatic complexity (number of execution paths within the file/function) of only 1.

v.1: 4.2.3.d v.2: 5.4.2.I	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS		SQL Scripts	1000	180	120	20	1320
			76%	14%	9%	2%	100.00%

Comment Related Instances/Discrepancies
Of the total 768 *VSS 2002* requirement non-compliances, 193 or 25% were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, functions with more than 5 levels

of indented scope, lines exceeding 80 characters, constants other than "0" or "1" not defined, incomplete header information, and non-unique module use.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 575 non-compliances or 75% of identified issues with 469 of those instances related to transaction updates within the database. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002.* The data supporting this review are found in Appendix B.

5.1.4 WinEDS 4.0 C# Source Code Review Results

WinEDS 4.0 consists of a C# component. The EDGE2*plus* and HAAT applications also contain the C# programming language. A total of 11,606 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 2882 discrepancies were identified and validated to be resolved. Those 2882 discrepancies encompassed 3719 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (2702) of those instances were comment related and the majority of the software related instances (529) were potential unhandled exceptions. The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified 7 files or functions that exceeded 240 eLOCs with the justification provided that these files/functions contained only variable initialization and had a cyclomatic complexity (number of execution paths within the file/function) of only 1.

v.1: 4.2.3.d v.2: 5.4.2.1	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS		C#	11324	234	57	7	11622
			97.4%	2%	0.5%	0.10%	100.00%

Comment Related Instances/Discrepancies
Of the total 3719 *VSS 2002* requirement non-compliances, 2702 or 73% were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, functions with more than 5 levels of indented scope, lines exceeding 80 characters, constants other than "0" or "1" not defined, incomplete header information, and non-unique module use.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 1017 non-compliances or 27% of identified issues. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002.* The data supporting this review are found in Appendix B.

5.1.5 WinEDS 4.0 VB 6.0 Source Code Review Results

WinEDS 4.0 consists of a Visual Basic 6.0 component. A total of 324 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 197

discrepancies were identified and validated to be resolved. Those 196 discrepancies encompassed 324 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (227) of those instances were comment related. The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified no files or functions that exceeded 240 eLOCs.

v.1: 4.2.3.d v.2: 5.4.2.1	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS		VB 6.0	348	28	5	0	381
			91.3%	7.4%	1.3%	0.0%	100.00%

Comment Related Instances/Discrepancies
Of the total 324 *VSS 2002* requirement non-compliances, 227 or 70% were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, functions with more than 5 levels of indented scope, lines exceeding 80 characters, constants other than "0" or "1" not defined, and incomplete header information.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 97 non-compliances or 30% of identified issues. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002.* The data supporting this review are found in Appendix B.

5.1.6 WinEDS 4.0 VB.Net Source Code Review Results

WinEDS 4.0 consists of a VB.Net component. A total of 1206 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 429 discrepancies were identified and validated to be resolved. Those 429 discrepancies encompassed 648 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (359) of those instances were comment related. The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified no files or functions that exceeded 240 eLOCs.

v.1: 4.2.3.d v.2: 5.4.2.1	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS		VB.Net	1143	38	1	0	1182
			96.7%	3.2%	0.1%	0.0%	100.00%

Comment Related Instances/Discrepancies
Of the total 648 *VSS 2002* requirement non-compliances, or 55%, were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, functions with more than 5 levels of indented scope, lines exceeding 80 characters, constants other than "0" or "1" not defined, and incomplete header information.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 289 non-compliances or 45% of identified issues. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002*. The data supporting this review are found in Appendix B.

5.1.7 WinEDS 4.0 Java Source Code Review Results

WinEDS 4.0 consists of the HAAT Listener which utilizes the Java coding language. A total of 476 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 152 discrepancies were identified and validated to be resolved. Those 152 discrepancies encompassed 200 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The majority (125) of those instances were comment. The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified no files or functions that exceeded 240 eLOCs.

v.1: 4.2.3.d v.2: 5.4.2.I	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS			463	7	1	0	471
		JAVA	98.3%	1.5%	0.2%	0%	100.00%

Comment Related Instances/Discrepancies
Of the total 200 *VSS 2002* requirement non-compliances, 125 or 63% were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Discrepancies noted variables without comments at the point of declaration, lack of in-line comments, lines exceeding 80 characters, incomplete header information, and lack of name readability.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 75 non-compliances or 38% of identified issues. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002*. The data supporting this review are found in Appendix B.

5.1.8 WinEDS 4.0 Assembly Source Code Review Results

WinEDS 4.0 consists of several Assembly source code components and languages. The Insight and Insight Plus APX and HPX as well as the MPR are written in Z80. Both the EDGE2*plus* and the HAAT assembler language components are written in 8051. VeriVote is PIC-ASM and the MBR bootloader which is association with the Edge II is in 80x86. A total of 1,219 files/functions were reviewed and all instances of non-conformance to the *VSS 2002* were validated to be closed. A total of 258 discrepancies were identified and validated to be resolved. Those 258 discrepancies encompassed 292 instances of *VSS 2002* requirements identified as not being met at the initial source code review.

The summary of the *VSS 2002* requirements and closure are as follows:

File Function Line Counts/Discrepancies
The file function line count results identified no files or functions that exceeded 240 eLOCs.

v.1: 4.2.3.d v.2: 5.4.2.1	**File's functions' line count**	On the Application level, no more than 50% exceeding 60 lines, no more than 5% exceeding 120 lines, and none exceeding 240 lines without justification.	**< 60**	**60 to 120**	**120 to 240**	**> 240**	**Total**
WinEDS		Assembly	1112	78	19	0	1209
			92.0%	6.4%	1.6%	0.10%	100.00%

Comment Related Instances/Discrepancies
Of the total 292 *VSS 2002* requirement non-compliances, 63 or 22% were rejected against the 15 comment-related requirements. All instances were noted in discrepancies; the comments were addressed by Sequoia, reviewed by iBeta, and validated to be closed. Due to the memory size of the chipset and the broad nature of the *VSS 2002* requirements for source code review, the ability to add comments to the Assembly source code was limited and recognized during the code review. As a result, a much smaller percentage of the source code discrepancies are comment related. Discrepancies noted included indentation, variables without comments at the point of declaration, lack of in-line comments, and constants other than "0" or "1" not defined.

Software Related Instances/Discrepancies
In reviewing the source code for the remaining 29 software related requirements, iBeta identified 229 non-compliances or 78% of identified issues. The majority of those instances, 173 or 75.5%, relate to the single entry or exit point requirement. All instances were noted in discrepancies, addressed by Sequoia, reviewed by iBeta, and validated to be closed.

The source code was found to meet the requirements of the *VSS 2002*. The data supporting this review are found in Appendix B.

5.2 *PCA TDP Document Review*

iBeta Quality Assurance reviewed all Sequoia Voting Systems submitted TDP documents of the WinEDS 4.0 voting system against the Vol. 2 Section 2 requirements of the *VSS 2002* (see Section Appendix C for a list of the reviewed documents). Each submitted document was reviewed against the specific section of the VSS applicable to that category of document. If the required content was present in one or more submitted documents results were summarized and the requirement was accepted. If it was not present the requirement was rejected.

Appendix C contains the specific review criteria for the TDP documents. Errors, nonconformities and anomalies observed in this review are summarized in Appendix E. Documentation of corrections and verification of corrections are contained in each summary.

Any instance of inconsistency in the version control of documents delivered by Sequoia Voting Systems was reported in Appendix E an informational issue.

5.2.1 PCA TDP Document Review Results

The documents of the Sequoia Voting Systems WinEDS 4.0 Technical Data Package were found to meet the requirements of Vol. 2 Section 2 of the *VSS 2002*. The data supporting this review are found in Appendix C.

5.3 *FCA Functional and System Integration Testing*

iBeta executed a review of the Sequoia WinEDS 4.0 voting system functionality to the requirements of the *VSS 2002* (see Appendix A). Tests covering system functional requirements were incorporated into eight standard system level integration test cases of end-to-end mock elections. Four of the tests were General Elections and four were Primary Elections. Election databases and ballots were prepared, installed, voted and reported exercising the input controls, error content, and audit message content of the voting system. The elections were programmed, voted and tallied to ensure ballot formats were accurately displayed, votes are accurately and reliably cast for the voting variations and functionality supported by the voting system. Effectiveness of security access controls, system integrity, availability, confidentiality and audit accountability were examined. The content and clarity of user instructions and processes was reviewed for usability. A General and a Primary election included visual and audio ballots as well as Spanish, English and Chinese. Votes were cast by testers with correctable visual disabilities to confirm that ballots can be accessed visually, aurally or with non-electronic dexterity aids in Spanish and English. Testing verified availability of screen contrast settings, ballot display settings, and required audio ballot controls. Content and accuracy of the Spanish translation was not tested. States and jurisdictions need to validate the content and accuracy of all translations.

The specific voting variations and system functions tested in the General and Primary Test Cases are identified in the Appendix D Test Methods. During the FCA Functional and System Level Testing numerous documentation and functional defects were noted. The functional discrepancies opened and closed in each test case are identified in the Appendix D Test Method. Sequoia resolved all identified defects. As appropriate, iBeta performed a document review and/or functional regression test. All regression testing was executed as an end-to-end system level test.

The testing was conducted on the system configuration identified in Section 3. System configuration was conducted in accordance with the Sequoia TDP that disables all non-specified services. The individual test iterations include identification of the specific software and firmware build versions in the Appendix D Test Methods. In accordance with *VSS 2002* Vol. 1 section 1.5, iBeta reviewed the body of knowledge deposited in the EAC's Voting System Reports Clearinghouse. The Test Plan delineates the Test Methods and the test steps executed to address those issues and concerns were executed during the FCA Functional and System Integration testing as well as the Security Test Case execution.

After all hardware and software testing was completed a final trusted build was performed with the release versions of the software and firmware (see Appendix G). This build was installed on the hardware configurations that had been utilized for Functional and System Integration testing. A full regression system integration test was performed on this final system configuration and is documented below.

5.3.1 Evaluation of Functional and System Integration Testing

Upon completion of all iterations of the Functional and System Level test cases, the Sequoia WinEDS 4.0 voting system was found to meet the Functional and System Integration requirements of the *VSS 2002*. Appendices A and D provide specific information on the FCA Functional and System Integration Testing. The defects encountered, their resolution and validations are listed in Appendix E.

5.3.2 Regression Functional and System Integration Testing

For the discrepancies that were functional defects and required software or firmware modifications, Sequoia submitted the modified source code, iBeta reviewed the code, performed a Trusted Build,

wrote end-to-end and system level test cases, and executed those test cases. Three full end-to-end test cases and 6 system level test cases were executed to validate all submitted fixes. These validations were recorded in the PCA and FCA Discrepancy Report.

In addition, the functionality of the EDGE2*plus* 305, which was not originally listed with the Sequoia Application to the EAC, was tested. At the conclusion of the regression testing, all functional defects were resolved.

5.4 *FCA Characteristics Testing (Recovery, Accessibility, Usability & Maintainability)*

iBeta re-used the General 4 Election that included audio, visual, and English ballots and the Primary 2 Election that was modified to included audio for this test. Test voting was performed by providing input direction to the voting machine touch screen and by using the Edge II Audio Voting Accessory (E-AVA) and the EDGE2*plus* Detachable Audio Voting Control (ABLE-D). Usability testing examined the functional capabilities addressing cognitive, perceptual, interaction, and privacy issues identified in VSS Vol.1 Section 3.1and RFI 2007-01. Accessibility testing examined the functional capabilities addressing visual, audio, dexterity, and mobility to confirm that the touch screen, E-AVA and the ABLE-D can be used to cast audio, visual, English ballots could be cast privately and independently on the Edge II and EDGE2*plus* units as identified in VSS Vol. 2 Section 3.2 and VSS Vol. 2 Section 6.5. Physical Characteristics and Design, Construction, and Maintenance requirements were tested on equipment, including the HAAT50, HAAT80, HAAT90, HAAT100, Card Activator, MPR and IMPR. Testing verified the functionality of screen contrast settings and text font ballot display settings, as well as the required audio ballot controls. All test conditions were in an ambient office environment. The Maintenance procedures outlined in the TDP were executed in conjunction with an examination of the physical characteristics and attributes of the Edge II, EDGE2*plus*, Insight, InsightPlus, and 400-C units to verify that they conformed to the requirements identified in VSS Vol. 2 Section 4.2 and 4.3.

During the test campaign, the EAC Decision on Request for Interpretation 2009-05 was issued. The test requirements associated with that RFI were incorporated into the Characteristics Test Case. The report from the third party laboratory that conducted the test is attached as H20 - Wyle Letter No. T57306B-002 dated January 11, 2010 subject of: Hearing Aid Compatibility Testing of the Sequoia Headset.

The testing was conducted on the system configuration identified in Section 3. The individual test iterations include identification of the specific software and firmware build versions in the Appendix D Test Methods. During testing 14 functional defects were noted. Their resolution and validations are identified in Appendix E.

5.4.1 FCA Characteristics Tests (Recovery, Accessibility, Usability & Maintainability)

The Sequoia WinEDS 4.0 voting system was found to meet the Recovery, Usability, Accessibility, Maintainability and Characteristics requirements of the *VSS 2002*. Appendices A and D provide specific information on the Characteristics (Maintainability, Usability and Accessibility) Testing. The defects encountered during the review, their resolution and validations are identified in Appendix E.

As dictated by RFI 2009-05, the COTS headset for the DREs was tested to the ANSI C63.19-2001 Category 4 Requirement by Wyle Laboratories and the results documented in Attachment H20 - Wyle Letter No. T57306B-002 dated January 11, 2010.

5.5 *FCA Security Review and Testing*

iBeta's security specialist, a Certified Information System Security Profession, supervised execution of a security analysis of the applicable TDP documents of the *VSS 2002 to* identify the threat model. First the analysis identified *VSS 2002* security requirements that were currently addressed in the standard testing, source code and document reviews. The analysis next identified any unique voting system specific tests, source code and document reviews that were needed. The tests, source code or documents reviews were traced to the *VSS 2002* requirement in the FCA Security Review and Testing

table. The results of the standard tests and reviews were recorded in the applicable FCA Functional and System Integration Testing, PCA Source Code Review or the PCA Document Review. The unique tests and reviews were documented in the FCA Security Review and Testing table. This documentation included the steps, acceptance and rejection criteria, and results. Appendix D contains the FCA Security Review and Testing table and the specific Test Methodology. During the test campaign, 98 discrepancies were encountered. The specific discrepancy numbers are identified in the Appendix D Security Review and Testing Method.

Of note during the security review, the three locks on the ballot bin of the Insight and InsightPlus were defeated with simple tools. Although any lock can be defeated over time and the lock provides for limited access, iBeta is disclosing this vulnerability within this final report.

In order to comply with the security test requirements identified in Vol. 2 Section 6.4 of the *VSS 2002*. iBeta approached security testing of the *VSS 2002* by first creating test scenarios which discounted the exposure to risk and excluded physical security procedures. However, in establishing acceptance and rejection criteria, iBeta assessed the potential exposure to risk and included physical security procedures as an acceptable security control, per the requirements of Vol. 1 Section 2.2.1 and 6.2 of the *VSS 2002*. To assess if an access control was effective iBeta considered the degree to which one or more of the following security controls was present: physical security procedures, password protection, detection in an audit, technical expertise required, obfuscation of sensitive material, and encryption of sensitive material. In determining potential exposure to risk the security specialist considered access from the user and if the exposure was from a trusted user or non-trusted user. Systems were accepted as meeting the security requirements of the *VSS 2002* if the security controls present were deemed effective to address the identified risk.

Testing was conducted on the system configuration identified in Section 3. The individual test iterations include identification of the specific software and firmware build versions in the Appendix D Test Methods.

5.5.1 FCA Security Review and Testing

Testing, source code and documentation reviews of the WinEDS 4.0 system found that the system met the applicable *VSS 2002* security requirements identified in the security analysis. Appendices A, B, C and D provide specific information on the FCA Security Review and Testing Failures, errors, nonconformities and anomalies observed in testing are summarized in Appendix E. Documentation of corrections and verification of corrections are contained in each summary.

5.6 *FCA Data Accuracy Testing*

The data accuracy requirements of the *VSS 2002* are addressed in all test cases. Any time a test required an election to be created, installed, voted, and/or reported the accuracy of the Sequoia WinEDS 4.0 voting system was being tested.

The FCA Accuracy Testing is specifically the Data Accuracy testing called out in Vol.2 section 4.7.1.1. This is a test performed in conjunction with the Temperature and Power Variations Test (v.2 section 4.7.1) and Reliability testing (v.2. section 4.7.3).

Data Accuracy Testing
The *VSS 2002* stipulates that a voting system fails if one error occurs before recording/reading 26,997 consecutive ballot positions correctly. A voting system must record/read 1,549,703 (or more) consecutive ballot positions correctly. If there's one error with more than 26,997 ballot positions but less than 1,549,703 correctly read, the test can be continued, with testing until another 1,576,701 consecutive ballot positions are counted without error (i.e. 3,126,404 with one error).

Temperature and Power Variations Testing & Reliability Testing
The *VSS 2002* stipulates that non-COTS precinct and central count systems must execute Data Accuracy testing in a chamber while operating for 48 hours in temperatures between 50° F and 95° F at varying voltage (see Appendix D Test Method). Reliability required a minimum operation of 163 hours. On February 6, 2008, the EAC issued Interpretation 2008-01 that identified the number of hours multiple

voting systems must accumulate. For this Sequoia test campaign, 2 units ran for 48 hours through Temperature and Power variations cycles and 36 hours at ambient. Operation included voting and tallying results at the rates prescribed in the *VSS 2002*. The equipment remained powered during all phases of test administration.

The testing was conducted on the system configuration identified in Section 3.

5.6.1 FCA Data Accuracy Tests (Accuracy, Reliability, Volume, & Stress)

The Sequoia WinEDS 4.0 voting system was found to meet the *VSS 2002* Vol. 1 Section 3.2.1 requirements. Appendices A and D provide specific information on the Data Accuracy Testing. No issues were encountered during this testing

5.7 *FCA Volume, Performance, Stress, and Error Recovery Testing*

iBeta executed a review of the Sequoia WinEDS 4.0 voting system limits to the requirements of the *VSS 2002* (see Appendix A). Tests covering system limit requirements were incorporated into three test cases of end-to-end mock elections. The test cases are Volume 1, Volume 1a, and Volume 2.

- Volume 1 and 1a objectives were to test and validate the ability to process, store and report data using the maximum number of ballot styles, contests, parties, candidate counters in an election and ballots/cards cast per machine within an election on different hardware configurations.
- Volume 2 objectives were to test and validate the ability to process, store and report data using the maximum number of active voting positions, parties, contests in a ballot style/precinct, precincts in an election, candidates per contest, ballot styles in a precinct, precincts in a memory pack, Vote For in a contest, and candidate counters in a precinct within an election on different hardware configurations.

Election databases and ballots were prepared, installed, voted and reported exercising the input controls, error content, and audit message content of the voting system. The elections were programmed, voted and tallied to ensure ballot formats were accurately displayed, votes are accurately and reliably cast and reported for the voting variations and functionality supported by the voting system.

5.7.1 FCA Volume (Performance, Stress, and Error Recovery) Tests

The Sequoia WinEDS 4.0 voting system was found to meet the Volume, Performance, Stress, and Error Recovery requirements of the *VSS 2002*. The specific voting variations and system limits tested in the Volume 1, Volume 1a, and Volume 2 Test Cases are identified in Appendix D section FCA Volume (Volume Stress, Performance and Error Recovery) Testing. During testing 3 functional defects were noted. Their resolution and validations are identified in Appendix E- Discrepancy Report.

5.8 *FCA Hardware Environmental Testing*

iBeta Quality Assurance executed environmental testing of the WinEDS 4.0 voting system in accordance with the *2002 VSS* requirements. The testing was conducted on the system configuration identified in Section 3 and in the attached hardware test reports by Criterion Technology, Inc., Wyle Laboratories, Oracle (formerly APT), and Intertek Testing Services.

The Sequoia WinEDS 4.0 vote scanning, counting and DRE voting equipment consists of the following:

- EDGE2*plus* CO.3
- EDGE2*plus* CO.4 with and without the VVPAT (as the VVPAT is not part of the federal certification test effort).
- EDGE2*plus* 305
- Edge II
- HAAT80, 90, and 100
- Insight
- Insight Plus
- Optech 400C
- WinEDS (COTS) with MPR

Additional voting system equipment that does not function in the role of vote scanning, counting, or DRE consists of the following components:

- HAAT50
- Card Activator
- iMPR

iBeta performed an examination of the COTS equipment Sycard PCCextend CardBus (PCMCIA adapter), APC Smart-UPS, Tash buddy buttons, HP LaserJet 1022n, Acer 17" Monitor, CyberPower CPS1500AVR UPS, headphones and various Laptops against the system specifications to confirm documented evidence of COTS equipment and operation per *VSS 2002* Vol.1 Section 4.1.2 and Interpretation 2007-05. iBeta confirmed that each COTS component had FCC Class 15B and CE marks affixed to each unit indicating that the product has been certified to meet these requirements and the COTS manufacturer's Declaration of Conformity confirming the manufacturer compliance claims.

Table 14 below lists the environmental test requirements and each piece of hardware with the corresponding test report. All of the 3rd party laboratory final reports are provided as attachments to this report including Wyle Letter No. T57306B-002 dated January 11, 2010 subject of: Hearing Aid Compatibility Testing of the Sequoia Headset.

During the federal test campaign, a number of Engineering Change Orders (ECOs) were submitted for hardware changes driven by testing. Those ECOs incorporated into the hardware configuration during the test campaign are identified in Table 14.

Engineering Change Order (ECO)	Hardware	Description
ECO-776	Insight/Insight Plus	Ferrites and tie wraps, copper coat valance, 2X holes, ground straps, Revision Level and EAC labels
ECO-777	MPR	Ferrite added
ECO-778	400-C	Ground wire, Rollback ECO 706 to previous , Revision Level label to 3.02P
ECO-2349	Edge II	Gray adapter added (replacement adapter for audio connector)
ECO-794	Edge II	Cover top of PCMCIA card with electrical liquid tape
ECO-795	Edge II	Increase size of LED to 7.9mm, install and silicone VVPAT LED cover
ECO-796	Edge II	Plastic cover over VVPAT & Audio connections
ECO-797	Edge II	New serial audio connector (spare part)
ECO-783	EDGE2*plus*	Install a washer to the key lock area
ECO-784	EDGE2*plus*	Remove excessive paint to improve ground contact
ECO-785	EDGE2*plus*	Add and glue hard plastic piece (5.5" x 4.5") to internal section of vent
ECO-786	EDGE2*plus*	Add grounding wire cable to internal section
ECO-3192	HAAT	Battery circuit saver
ECO-787	HAAT	Add copper paint to key lock area
ECO-788	HAAT	Grounding reinforcement of the LCD circuit
ECO-789	HAAT	Add polycarbonate frame between the LCD screen and the keypad membrane
ECO-790	HAAT	Cover membrane connection wire with a heat shrink tube
ECO-791	HAAT	Bend cable in new direction and maintain position with a rubber band
ECO-792	HAAT	Circuit configuration to improve battery life
ECO-798	Edge II	Ground Wire

Table 14: Engineering Change Orders

Equipment	Summary of Testing Conducted	MIL-STD 810D						FCC								OSHA
		516.3 Bench Handling	514.3 Category 1 Vibration	502 Low Temp	501 High Temp	507-2 Humidity	501 & 502 Temp & Power Variation With Accuracy & 163 hour Reliability Tests	Electromagnet Radiation Part 15 Class B	Power Disturbance 61000-4-11	Electrostatic Disruption 61000-4-2	Electromagnetic Susceptibility 61000-4-3	Electrical Fast Transit 61000-4-4	Lightening Surge 61000-4-5	RF Immunity 61000-4-6	Magnetic Fields Immunity 61000-4-8	Safety Title 29, Part 1910
EDGE2*plus* CO.3 and CO.4	EDGE2*plus* CO.3 and CO.4 both audio and flash drive .The CO.4 is the CO.3 hardware configuration plus the CO.4 change order. ESD tested with and without the VVPAT.	10	10	10	10	10	24	23	11, 12	23, 25	23	23	11, 12	23	11, 12	6
EDGE2*plus* 305	The 305 is the CO.4 without audio and with ECRE2PMAINN24-090831	10	10	10	10	10	24	23	11, 12	23	23	23	11, 12	23	11, 12	6
HAAT50 A0.3 and A1.1 HAAT 80 A1.1 HAAT90 A1.1	The HAAT50 is not vote scanning or counting equipment. HAAT 50 is the HAAT80 without the printer and the HAAT80 is hardware equivalent of the HAAT90 (difference is a modem in the HAAT90).	7	7	7	7	7	24	21	7	21	7	5	5	5	5	7
HAAT100 A0.7		7	7	7	7	7	24	22	22	22, 25	22	22	22	22	22	7
HAAT100 A0.7	With Battery Circuit Saver	7	7	7	7	7	24	22	22	22, 25	22	22	22	22	22	7
IMPR A1.0 and C1.1	The iMPR was tested in conjunction with HAAT100. The IMPR is not vote scanning or counting equipment.	7	7	7	7	7	24	22	22	22, 25	22	22	22	22	22	7
MPR Revision D		1	1	1	1	1	17	13	13	13	13,17	13	13	13	13	17
Edge II with VeriVote and audio		8	8	8	8	8	24	9	9	25	9	9	9	9	9	9
Insight with UPS		2	2	2	2	2	19	14	14	14	14	14	14	14	14	2
Insight Plus with UPS		2	2	2	2	2	19	15	15	15	15	15	15	15	15	2
400-C with UPS		3	3	3	3	3	18	16	16	16	16	16	16	16	16	3
Card Activator	The Card Activator is not vote scanning or counting equipment.	8	8	8	8	8	8	9	9	9	9	9	9	9	9	9

Table 15: Matrix of Environmental Hardware Testing Results Reports

Test Reports per EAC 24 July 2009 letter on test results reuse of hardware testing from the Sequoia WinEDS 4.0.034 test campaign:

1. Wyle Laboratories Report No. 50932-03 Qualification Testing of the Memorypack Receiver dated 10 May 2005.
2. Wyle Laboratories Report No. 52125-02 Hardware Qualification Testing of the Optech Insight/Insight Plus dated 16 March 2006.
3. Wyle Laboratories Report No. 52125-04 Hardware Qualification Testing of the Sequoia Optech 400-C Ballot Counter with WinETP dated 16 March 2006

Test Reports per EAC 29 September 2009 letter on test results reuse of hardware testing from the Sequoia WinEDS 4.0.034 test campaign:

4. EDGE2*plus* CO3: Percept Technology Labs Test Report dated 7/18/2006
5. HAAT: Criterion Technology Report Number 060608-1056 EMC Qualification Test Report Hybrid Activator, Accumulator and Transmitter, HAAT90 dated 5 July 2006
6. Components Reliability & Safety, Inc. Report #06-1000 Product Safety Testing and Evaluation for Voting Machine Model number Edge 2 Plus-200, -300 22 June 2006
7. HAAT 90 Percept Technology Labs Test Report dated 7/17/2006
8. Wyle Laboratories Report No. 51884-03 Hardware Qualification Testing of the Edge Models I & II DRE Voting Machines, VeriVote Printer, Card Activator, and ADA Audio Adapter Peripherals dated 16 March 2006
9. Wyle Laboratories Report No. 44733-02 CE Verification Testing on the AVC Edge Voting Machine, Card Activator and Audio Box dated 23 April 2002
10. APT Testing Services Report for Testing of Sequoia Edge 2 Plus 200 5/16/-6-6/12/06

Test Report s identified as reuse per the WinEDS v. 4.0 VSTL Test Plan:

11. Criterion Technology Report Number 060509-1038 EMC Qualification Test Report Sequoia Voting System, Edge2plus 200 dated 31 May 2006 (ALL EMI/EMC)
12. Criterion Technology Report Number 060608-1057 EMC Qualification Test Report Sequoia Voting System, Edge2plus 300 dated 5 July 2006 (ALL EMI/EMC for the updates from 200 to 300)

Test Reports issued during this current Sequoia Test Campaign:

13. Criterion Technology Report Number 080904-1302 EMC Qualification Test Report MPR, 3.01 Rev E dated 24 June 2009
14. Criterion Technology Report Number 080904-1310 EMC Qualification Test Report Insight, G.05 dated 17 June 2009
15. Criterion Technology Report Number 080904-1335 EMC Qualification Test Report Insight Plus, A.05 dated 29 June 2009
16. Criterion Technology Report Number 080904-1338 EMC Qualification Test Report Optech 400-C, 3.02P dated 29 June 2009
17. Wyle Laboratories Report No. T56534-01 Hardware Testing and Evaluation of the Sequoia Voting Systems Optech MemoryPack Receiver dated 23 November 2009
18. Wyle Laboratories Report No. T56534-02 Hardware Testing and Evaluation of the Sequoia Voting Systems Optech 400-C Ballot Counter dated 23 November 2009
19. Wyle Laboratories Report No. T56534-03 Hardware Testing and Evaluation of the Sequoia Voting Systems Optech Insight and Insight Plus Precinct Ballot Counter dated 23 November 2009
20. Wyle Letter No. T57306B-002 dated January 11, 2010 subject of : Hearing Aid Compatibility Testing of the Sequoia Headset
21. Criterion Technology Report Number 090929-1472 EMC Qualification Test Report HAAT90 Rev 1 dated 16 June 2010
22. Criterion Technology Report Number 090929-1475 EMC Qualification Test Report HAAT100 Rev 1 dated 24 June 2010
23. Criterion Technology Report Number 090929-1474 EMC Qualification Test Report Edge2plus Rev 2 dated 15 July 2010
24. Oracle® Advanced Product Testing Lab Testing Services Report 10-00317 dated 25 March 2010
25. Intertek Electronic Voting Machine and Voter Card reader Test Report, 100097216DEN-001, 06/05/2010

5.8.1 FCA Hardware Environmental Tests

The Sequoia WinEDS 4.0 voting system was found to meet the environmental testing conducted in accordance with *VSS 2002* Vol.1 Section 3.2.2.5 through 3.2.2.12. As the *VSS 2002* requires DRE's to include audio functionality the environmental tests which require performance while the unit is operating must include audio operations, the Environmental Operating Tests therefore included both visual and audio ballot operations. Appendix D details specific information on the Hardware Environmental Testing. Failures, errors, nonconformities and anomalies observed in testing are summarized in Appendix E- Discrepancy Report. Documentation of corrections and verification of corrections are contained in each summary. During testing 18 functional defects were noted. Any mitigation required was performed in compliance with Section 2.5.2.1.3 of the EAC Laboratory Accreditation Program Manual.

5.9 *FCA Telephony and Cryptographic Review and Testing*

The WinEDS 4.0 voting system uses telephony to transmit unofficial consolidated results by wired and wireless modem from the Hybrid Activator, Accumulator and Transmitters (HAAT90 and HAAT100) to the central count WinEDS receiving server endpoint (HAAT Listener). The HAAT90 and HAAT100 perform their accumulator role to consolidate precinct results prior to transmission. iBeta Quality Assurance executed the consolidation and transmission steps of General 2 (HAAT90) and General 3 or Primary 1 (HAAT100) test cases to specifically test the Telephony and Cryptographic aspect of the WinEDS 4.0 voting system. The testing was conducted on the system configuration identified in Section 3.

5.9.1 FCA Telephony and Cryptographic Review and Tests

iBeta confirmed that the WinEDS 4.0 voting system election management hardware and installation procedures reflect the configuration described in Section 3. The HAAT90 and HAAT100 are prepared with ballot definitions at a secure location and transported to the precinct locations. After the election, the HAAT90 and HAAT100 upload consolidated results by modem. The HAAT90 utilizes a POTS modem with an endpoint to the RAS which in turn sets up a TCP/IP connection to the HAAT Listener. The RAS consists entirely of COTS components. The HAAT100 utilizes a wireless connection to a COTS WAN with a TCP/IP endpoint at the HAAT Listener (both systems have a firewall between the public network and the HAAT Listener). In fielded systems, the COTS WAN is generally a state-wide or county-wide network. iBeta simulated this network utilizing the Internet. Wireshark was used to monitor the communications in a local environment to compare to the transmissions at the TCP/IP network layer. All communications are protected by formation of a TLS (https) connection between the HAAT90 or HAAT100 and the HAAT Listener. In addition to the TLS connection, the HAAT devices utilize AES encryption and a pre-shared election-specific key to transmit the consolidated vote data. Modem transmissions were monitored at the TCP/IP layer and a Mini-Maxwell device served as a man-in-the-middle (MITM) to delay, reorder, drop and duplicate packets transmitted in the system. Appendix D details specific information on the Telephony and Cryptographic Review and Testing. Failures, errors, nonconformities and anomalies observed in testing are summarized in Appendix E. Documentation of corrections and verification of corrections is contained in each summary.

6 Opinions & Recommendations

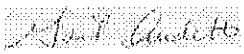
iBeta Quality Assurance has completed the testing of Sequoia WinEDS 4.0 Voting System. All testing prescribed in the test plan or amended test plan was performed as identified. Documentation of any divergence from the EAC approved test plan was included in the amended as-run test play (see Appendix H). All identified anomalies or failure were reported and resolved. The information provided in this report is an accurate representation of the certification test effort of the Sequoia WinEDS 4.0 Voting System. It is our opinion that the report is complete.

For disclosure, iBeta is noting that the VVPAT association with the EDGE2*plus* was included in the test campaign although it is not part of the federal certification test effort (see Discrepancy #111 for details pertinent to this issue).

Based on the findings identified in Section 5, it is our opinion that the acceptance requirement of the *Federal Election Commission Voting System Standards* April 2002 and the Dominion manufacturer specifications have been met for the hardware, software and user documentation of the system configuration submitted for certification testing.

iBeta Quality Assurance recommends that the Election Assistance Commission certifies Sequoia WinEDS 4.0.

See Appendix K for information regarding the EAC Certification number.



Gail Audette
Quality Manager
iBeta Quality Assurance

7 APPENDICES: TEST OPERATION, FINDINGS & DATA ANALYSIS

The *Voting System Test Laboratory Program Manual v.1.0* Appendix B identifies content in specific appendices. In order to ensure that this content and content required by *VSS 2002* Volume 2 Appendix B a trace is provided in section 1.4 to clarify the location of this specified content.

7.1 *Appendix A: Certification Test Requirements*

Appendix A identifies the test results to the Certification Test Requirement of the *VSS 2002*. Requirements are marked as follows:

- Accept: met the *VSS 2002* requirement
- Reject: did not meet the *VSS 2002* requirement
- NA: the requirement is not applicable to the voting system type submitted for Certification Testing
- Pending: *VSS 2002* requirements that cannot be completed by the VSTL until after Certification
- Out of Scope: *VSS 2002* requirements which are performed by entities other than the VSTL

Requirements marked Reject, NA, Pending or Out of Scope shall include an explanatory note. (Example: If a voting system is only a Central Count Scanner, the requirement is marked "NA" and a comment indicates "Not a DRE.") The test case trace corresponds to the Test Methods identified in the Appendix H- Amended Test Plan and Appendix D- FCA Testing.

- Env - Environmental Test Case
- Char - Characteristics Test Case
- G1 - General Election 01 Test Case
- G2 - General Election 02 Test Case
- G3 - General Election 03 Test Case
- G4 - General Election 04 Test Case
- P1 - Primary Election 01 Test Case
- P2 - Primary Election 02 Test Case
- P3 - Primary Election 03 Test Case
- P4 - Primary Election 04 Test Case
- G3R - General Election 03 Regression Test Case
- G4R - General Election 04 Regression Test Case
- P1R - Primary Election 01 Regression Test Case
- P2R - Primary Election 02 Regression Test Case
- P3R - Primary Election 03 Regression Test Case
- T&C - Telephony and Cryptographic Test Case
- Sec - Security Test Case
- Acc - Accuracy Test Cases
- Vol1 - Volume 01 Test Cases
- Vol2 - Volume 02 Test Case
- VolR - Volume Regression Test Case

Optional requirements which apply to the voting system type but are not supported by the WinEDS 4.0 voting system are not marked "NA". Instead they are marked "Accept", with an explanatory comment. The reason for this is to provide a positive identification that iBeta reviewed the voting system for all applicable requirements, including this optional functionality and confirmed non-support. (Example: If a voting system does not have a VVPAT. The requirements are marked "Accept" and a comment indicates "DRE does not have a VVPAT".)

Issues identified during testing are cross-referenced to the Appendix E- Discrepancy Report.

EAC Decisions on Requests for Interpretation which were applicable to the voting system submitted for certification testing are noted in the comments.

Due to the size of this Appendix, it is provided as an attachment. To view, select **Attachments** in the **View** menu in Adobe.

7.2 *Appendix B: PCA Source Code Review*

The PCA Source Code Review was conducted against the following requirements in the *VSS 2002* (those highlight in green are comment related):

VSS	Requirement	Definition
Vol. 1 Section 4.2.2-Integrity		
v.1: 4.2.2	**Self-modifying code**	Self-modifying, dynamically loaded, or modification of compiled or interpreted code is prohibited
Vol. 1 Section 4.2.3- Modularity		
v.1: 4.2.3.a	**Specific function**	Module performs a specific function
v.1: 4.2.3.b	**Module has unique name**	Uniquely and mnemonically named using names that differ by more than a single character
v.1: 4.2.3.b 4.2.7 (a, a.1-a.6)	**Module has header**	Header describes purpose, other units needed, inputs, outputs, files read or written, globals, revision records (for modules greater than 10 lines) Header comments shall provide the following information: 1) The purpose of the unit and how it works; 2) Other units called and the calling sequence 3) A description of input parameters and outputs 4) File references by name and method of access 5) Global variables used 6) Date of creation and a revision record
v.1: 4.2.3.c	**Required resources**	All required resources, such as data accessed by the module, should either be contained within the module or explicitly identified
v.1: 4.2.3.e	**Single Entry Point**	Module has a single entry point
v.1: 4.2.3.e	**Single Exit Point**	Module has a single exit point
v.1: 4.2.3.f	**Control structures**	Support the modular concept and apply to any language feature where program control passes from one activity to the next.
Vol. 1 Section 4.2.4-Control Constructs		
v.1: 4.2.4.a	**Acceptable Constructs**	Acceptable constructs are Sequence, If-Then-Else, Do-While, Do-Until, Case, and the General loop (including the special case for loop);
v.1: 4.2.4.b	**Vendor Defined Constructs with Justification**	If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable control structure logic). The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution
v.1: 4.2.4.c	**Execution through Control Constructs**	While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs.
v.1: 4.2.4.d	**Program re-direction**	Logic that evaluates received or stored data shall not re-direct program control
Vol. 1 Section 4.2.5-Naming Conventions		
v1: 4.2.5.a	**Name Readability**	Names shall be selected so that their parts of speech represent their use.
v.1: 4.2.5.b 4.2.5.c	**Class, function and variable names**	Consistent names are used. Names shall be unique within an application and differ by more than a single character.
v.1: 4.2.5.d	**Keyword**	Keywords shall not be used as names of objects, functions, procedures, or variables
Vol. 1 Section 4.2.6-Coding Conventions		
v.2: 5.4.2.a	**Uniform calling sequences**	Uses uniform calling sequences.
v.2: 5.4.2.a	**Parameters type and range validation**	All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the types and ranges
v.2: 5.4.2.b	**Explicit return values**	The return is explicitly defined for functions and explicitly assigned
v.2: 5.4.2.c	**Macros**	Does not use macros that contain returns or pass control beyond the next statement
v.2: 5.4.2.d	**Unbound arrays**	Provides controls to prevent writing beyond the array, string, or buffer boundaries
v.2: 5.4.2.e	**Pointers**	Provides controls that prevent pointers from being used to overwrite executable instructions or to access areas where vote counts or audit records are stored
v.2: 5.4.2.f	**Case statements**	Default choice explicitly defined

VSS	Requirement	Definition
v.2: 5.4.2.g	**Vote counter overflowing**	Provides controls to prevent any vote counter from overflowing
v.2: 5.4.2.h	**Indentation**	Code is indented consistently and clearly
v.2: 5.4.2.j	**Code generator**	Generated code should be marked as such with comments defining the logic invoked
v.2: 5.4.2.k	**Line length**	No line of code exceeding 80 columns in width without justification
v.2: 5.4.2.l	**Executable statement**	One executable statement for each line of source code
v.2: 5.4.2.m	**Embedded executable statement**	The single embedded statement may be considered a part of the conditional expression. Any additional executable statements should be split out to the other lines.
v.2: 5.4.2.n	**Mixed-mode operations**	Avoids mixed-mode operations. Comment if mixed-mode usage is necessary.
v.2: 5.4.2.o	**Exit() message**	Upon exit() at any point, presents a message to the user indicating the reason for the exit ().
v.2: 5.4.2.p	**Format of messages**	Separate and consistent formats to distinguish between normal status and error or exception messages
v.2: 5.4.2.q	**References variables**	References variables by fewer than five levels of indirection (i.e. a.b.c.d or a[b].c->d)
v.2: 5.4.2.r	**Levels of indented scope**	Functions with fewer than six levels of indented scope
v.2: 5.4.2.s	**Variable initialization**	Initializes every variable upon declaration where permitted.
v.2: 5.4.2.t	**Explicit Comparisons**	Explicit comparisons in all if() and while() conditions.
v.2: 5.4.2.u	**Constant Definitions**	All constants other than "0" and "1" defined or enumerated
v.2: 5.4.2.v	**Ternary Operator**	Only contains the minimum implementation of the "a = b ? c : d" syntax. Expansions such as "j=a?(b?c:d):e;" are prohibited.
v.2: 5.4.2.w	**Assert() statement**	All assert() statements coded such that they are absent from a production compilation
Vol. 1 Section 4.2.7 -Comments		
v.1: 4.2.7.b	**Variables**	All variables shall have comments at the point of declaration
v.1: 4.2.7.c	**In-Line Comments**	In-line comments shall be provided to facilitate interpretation of functional operations, tests, and branching
v.1: 4.2.7.d	**Assembly code**	Assembly code shall contain descriptive and informative comments
v.1: 4.2.7.e	**Comments in uniform format**	All comments formatted in a uniform manner
Vol. 1 Section 6.4.2 -Protection Against Malicious Software		
v.1: 6.4.2	**Malicious Software**	Susceptibility to file or macro viruses, worms, Trojan horses, logic bombs, or hardcoded passwords

The summary of the instances noted against the software related *VSS 2002* requirements listed above for each source code language along with the iBeta validation is listed in a CONFIDENTIAL Appendix B provided as an attachment.

7.3 *Appendix C: PCA TDP Document Review*

The PCA TDP Document review, to the requirements of the *VSS 2002 section 2*, was performed by iBeta.

Due to the size of this Appendix, it is provided as an attachment. To view, select **Attachments** in the **View** menu in Adobe.

7.4 *Appendix D: FCA Test Results*

7.4.1 FCA Functional and System Level Testing

7.4.1.1 *Functional Test Results*

The system configurations identified below represent the test platform detail (including serial numbers, if applicable) for the associated functional test cases. A separate appendix contains detail and results. Due to the size of this Appendix, it is provided as an attachment. To view, select **Attachments** in the **View** menu in Adobe.

Voting System Test Matrix

General 1	General 2	General 3	General 4	WinEDS 4.0 Hardware	Primary 1	Primary 2	Primary 3	Primary 4
CO	MI	IL	PA	State	WA	WI	AZ	IL
39349	36273		39349	Edge II	39349	36273	36273	
28400			28400	VeriVote Printer (Rev C)	28400	28400	384VVPTB 00002551	
	3016976			Seiko DPU-414 Printer			3016976	
			X	Edge Audio Voting Accessory (Rev D)				
			X	Edge AUX Power Unit				
				Card Activator (Rev D)			02144147 HCM	
06323446 HCM				Card Activator (Rev E)				
	5472	9880		EDGE2*Plus* (C0.3) Model 300		9880		9880
S10001		S10001	S10001	EDGE2*Plus* (C0.4) Model 300	S10001		S10002	S10001
				EDGE2*Plus* (C0.4) Model 305				
X	X	X	X	APS (UTG300) Printer	X	X	X	X
			512029	Insight (G05)	501751		501751	
502918	502918	502918	502896	Insight Plus (A05)	502896	502918		502918
various	various	various	various	MemoryPack	various	various	various	various
PR506777	PR506777	500607	500607	MPR (Rev D)	500607	500607	PR506777	500607
200208		200208		400-C (3.0xP)	200208	200208		200208
				IMPR (A1.0)				
577IMPRC 1105908	577IMPR C1105908	577IMPR C1105907		IMPR (C1.1)				577IMPR C1105907
				HAAT50 (A0.3)		1045		
			351HT50A 11001008	HAAT50 (A1.1)	351HT50A 11001008			
1197				HAAT80 (A1.1)				
	1138			HAAT90 (A1.1)				
		4464		HAAT100 (A0.7)				4464
	X	X		HAAT Listener				X
	X			RAS Server				

Voting System Test Matrix Regression Round 1

General 1	General 2	General 3	General 4	WinEDS 4.0 Hardware	Primary 1	Primary 2	Primary 3	Primary 4
CO	MI	IL	PA	State	WA	WI	AZ	IL
39349	36273		39349	Edge II	39349	36273		
28400			X	VeriVote Printer (Rev C)	X	12524		

	3016976			Seiko DPU-414 Printer		
			3427	Edge Audio Voting Accessory (Rev D)		
				Edge AUX Power Unit		
				Card Activator (Rev D)		
06323446 HCM				Card Activator (Rev E)		06348746 HCM
		5472		EDGE2*Plus* (C0.3) Model 300	5472	5472
S10001			S10001	EDGE2*Plus* (C0.4) Model 300		S10001
	100809			EDGE2*Plus* (C0.4) Model 305		
X	X			APS (UTG300) Printer	X	X
	501751			Insight (G05)	501751	
502918				Insight Plus (A05)		502918
various	various			MemoryPack	various	various
PR506777	PR506777			MPR (Rev D)	PR506777	500607
200208		200227		400-C (3.0xP)	200227	
	350IMPRA 10003191			IMPR (A1.0)		
577IMPRC 1105908				IMPR (C1.1)		577IMPR C1105904
				HAAT50 (A0.3)		
				HAAT50 (A1.1)		
1197				HAAT80 (A1.1)	1197	
	334HT90A 11001128			HAAT90 (A1.1)		
				HAAT100 (A0.7)		357H100 A0700617 7
	X			HAAT Listener		X
	X			RAS Server		

7.4.1.2 *System Level Test Results*

Please see the Voting System Test Matrix above as corresponds to each rerun (versioned) test case. Discrepancies were noted in Appendix E - Discrepancy Report.

7.4.1.3 *Security Review and Test Results*

Please see the Voting System Test Matrix above as corresponds to general test cases referenced in the Security test steps. Discrepancies were noted in Appendix E - Discrepancy Report.

7.4.2 FCA Accuracy Testing

Accuracy Tests were conducted at APT and Wyle. The system configurations identified below represent the test platform detail (including serial numbers, if applicable) for the associated Accuracy Test Cases. Discrepancies were noted in Appendix E - Discrepancy Report.

Location of Equipment	Test Case	Description of Equipment	Serial Number
APT	DRE Accuracy	Dell Laptop Model D630 #PP18L Duo T9300 @ 2.50GHz 3.50 GB RAM	Service Tag: 545WXG1
APT	DRE Accuracy	HAAT90	1128
APT	DRE Accuracy	HAAT100	4464

APT	DRE Accuracy	HAAT100	4412
APT	DRE Accuracy	Edge II	39349
APT	DRE Accuracy	Edge II	36273
APT	DRE Accuracy	EDGE2*plus* Model 300 Rev. C0.3	5472
APT	DRE Accuracy	EDGE2*plus* Model 300 Rev. C0.3	9880
APT	DRE Accuracy	EDGE2*plus* Model 300 Rev. C0.4	S10001
APT	DRE Accuracy	EDGE2*plus* Model 305 Rev. C0.4	100809
Wyle	Optical Scan Accuracy	400-C Central Count	200226
Wyle	Optical Scan Accuracy	400-C Central Count	200227
Wyle	Optical Scan Accuracy	Optech Insight	501751
Wyle	Optical Scan Accuracy	Optech Insight	512029
Wyle	Optical Scan Accuracy	Optech InsightPlus	502896
Wyle	Optical Scan Accuracy	Optech InsightPlus	502918
iBeta	Volume 1/1A	Edge II	31172
iBeta	Volume 1/1A	Optech Insight	501751
iBeta	Volume 1/1A	Optech Insight	512029
iBeta	Volume 1/1A	EDGE2*plus* Model 300 Rev. C0.3	9880
iBeta	Volume 1/1A	Optech Insight Plus	502918
iBeta	Volume 1/1A	Optech Insight Plus	502896
iBeta	Volume 1/1A	HAAT100	4464
iBeta	Volume 1/1A	Optech 400C Optical Scanner	200208
iBeta	Volume 1/1A	Optech 400C Optical Scanner	200226
iBeta	Volume 2	Optech Insight	501751
iBeta	Volume 2	Optech Insight Plus	502896
iBeta	Volume 2	Edge II	36273
iBeta	Volume 2	EDGE2*plus* Model 300 Rev. C0.4	S10002
iBeta	Volume 2	EDGE2*plus* Model 300 Rev. C0.3	5472
iBeta	Volume 2	HAAT90	1138
iBeta	Volume 2	IMPR Rev.C 1.1	577IMPRC1105904
iBeta	Volume 2	MPR Rev D	PR506777
iBeta	Volume 2	400-C (3.02P)	200226

7.4.3 FCA Maintainability, Usability and Accessibility Testing

Please see the Voting System Test Matrix above for system configurations identified for the test platform for the Characteristics test case as corresponds to general and primary test cases referenced in the test case. Discrepancies were noted in Appendix E - Discrepancy Report.

7.4.4 FCA Hardware Environmental Testing

The system configurations identified below represent the test platform detail (including serial numbers, if applicable) for the Environmental Test Case. Discrepancies were noted in Appendix E - Discrepancy Report.

Description of Equipment	Serial Number
HAAT 90	334HT90A11001128
IMPR Rev. A1.0	350IMPRA10003191
IMPR Rev. C 1.1	577IMPRC1105917
HAAT 100	4412
HAAT 100	6177
IMPR Rev. C 1	5914
HAAT 100	4412

EDGE2*plus* C0.4	S10004
Edge II	51178
VVPAT for Edge2	12524
E-AVA & Headset	3422
EDGE2*plus* C0.4	S10002
Memory Pack Receiver (MPR) Rev D	PR506801
Memory Pack Receiver (MPR) Rev E	PR506777
(8) Power Sonic Class 2 Automatic Battery Charger PSC-12800A-C 12 volt-800mA	PR506801
Optech Insight G05	512029
CyberPower CPS1500AVR (400-C UPS)	BB07Y2000347
400-C (3.02P)	200227
Optech Insight Plus A05	502918
400-C (3.02P)	200226
Optech Insight Plus A0.2 (surface mount)	514044
Optech Insight G05	501751
Optech Insight Plus A05	502896
Optech Insight A.02 (surface mount)	502891
APC UPS (COTS)	No SN identified
APC Smart-UPS 2200 (black) (SUA2200) (COTS)	J50644088202

7.4.5 FCA Telephony and Cryptographic Review and Testing

Please see the Voting System Test Matrix above for system configurations identified for the test platform for the Telephony and Cryptographic test case as corresponds to general and primary test cases referenced in the test case. Discrepancies were noted in Appendix E - Discrepancy Report.

7.5 *Appendix E: Discrepancy Report*

Due to the size of this Appendix, it is provided as an attachment. To view, select **Attachments** in the **View** menu in Adobe.

7.6 *Appendix F: Warrant of Accepting Change Control Responsibility*

dominion VOTING

215 Spadina Avenue
Toronto, ON M5T 2C7
Tel: 416-762-8683
Fax: 416-762-8663

August 3, 2010

Ms. Gail Audette
Quality Manager
iBeta Quality Assurance
2675 South Abilene Street, Suite 300
Aurora, Colorado 80014

Re: Dominion Voting Systems Warrant of Accepting Change Control Responsibility as defined in Appendix B of the EAC VSTL Program Manual and NOC 09-004

Ms. Audette:

In accordance with the above referenced US Election Assistance Notice of Clarification:

Dominion Voting Systems warrants that any and all changes made to the WinEDS 4.0 voting system during the test campaign will be incorporated to any deployed voting system and its components prior to the application of any sort of mark of EAC Certification to that deployed system or its components.

Do not hesitate to contact me if you have any questions with respect to this Warrant.

Sincerely,
Edwin B. Smith, III
Vice President, Certification and Compliance
Dominion Voting Systems Corporation
Tel: (416) 762-8683 ext. 271
Fax: (416) 762-8663

dominion VOTING

7.7 Appendix G: Trusted Builds WinEDS 4.0 Voting System

The Sequoia WinEDS 4.0 voting system is composed of the hardware, software, and documents identified in section 3.

iBeta uses a COTS hash program (Maresware) to obtain File Size, MD5 and SHA1 hashes during trusted builds. Both algorithms have been validated using the test data from the NIST NSRL website (http://www.nsrl.nist.gov/testdata/). This program is widely used in forensic analysis of systems and also used by some states to verify their voting software. The MD5 and SHA1 hashes are taken to be consistent with the currently distributed NSRL data files which contain the hash resulting from each of those two algorithms.

Listed below are the source code versions reviewed by iBeta for the Final Trusted Builds versions of the Sequoia WinEDS 4.0 voting system (NIST Handbook 150-22 4.2.3, 4.13.2, 4.13.4, 5.10.4 VSS Vol. 1: 9.6.2.4). The final Trusted Build was utilized for the full end-to-end regression test in accordance with the requirements of the Section 5.6.3.4 of the EAC Testing and Certification Program Manual.

Due to the size of this Appendix, it is provided as an attachment. To view, select **Attachments** in the **View** menu in Adobe.

7.7.1 Trusted Build ICR (iMPR) and TSMPlayer (March 29, 2010)

7.7.2 Trusted Build HAAT_OS (April 5, 2010)

7.7.3 Trusted Build EDGE2*plus*_OS (April 15, 2010)

7.7.4 Trusted Build HAAT Listener, HAAT Installer, and Saes_Log (April 16, 2010)

7.7.5 Trusted Build P168 and 3200 Controller (April 26, 2010)

7.7.6 Trusted Build EDGE2*plus* (May 5, 2010)

7.7.7 Trusted Build Insight, MPR, and VVPAT (May 19, 2010)

7.7.8 Trusted Build ABU (May 20, 2010)

7.7.9 Trusted Build Card Activator (June 2, 2010)

7.7.10 Trusted Build Edge II (July 9, 2010)

7.7.11 Trusted Build HAAT Application (July 9, 2010)

7.7.12 Trusted Build WinEDS and WinETP (September 2, 2010)

7.8 *Appendix H: Amended Test Plan*

The approved test plan along with the EAC Approval Letter dated 23 April 2009 are located on the EAC website.

This test plan was amended during test execution. This amended test plan is attached, *Sequoia Voting System, WinEDS v.4.0 VSTL Certification Test Plan v.4.0.* Changes are provided in purple text for easy identification.

7.9 *Appendix I: State Test Reports*

During the federal certification test campaign of WinEDS 4.0, iBeta conducted three separate state testing efforts and a summary of the results of those test projects are provided below. In accordance with the EAC Notice of Clarification 2007-03, a separate test plan for each test effort was created as a stand-alone document. Concurrent state testing was conducted during the EAC testing and certification test campaign; however, the concurrent state testing is not subject to EAC Certification or oversight. The State test reports addressed only the functionality associated with the State specific configuration of the WinEDS 4.0 system as defined in the Sequoia TDP.

7.9.1 City and County of San Francisco

The focus of this test effort was on the Ranked Choice Voting (RCV) functionality of WinEDS 4.0. The test effort start date was 25 April 2008. A separate test plan was submitted and approved by the vendor prior to test initiation. The test effort was completed on 4 August 2008 with the approval of the Test Report.

iBeta completed the functional testing of the Sequoia Voting Systems WinEDS v.4.0 with WinETP and San Francisco Rank Choice Voting (RCV) as outlined in alternative implementation Section 2.3 of the *Sequoia Voting Systems Ranked Choice Voting Alternative Implementations for California* document version 1.00 dated April 2008 and the approved *City and County of San Francisco Ranked Choice Voting (RCV) Test Plan* v2.0 dated 19 June 2008 which identified iBeta Quality Assurance's (iBeta) approach to functional testing of the Sequoia Voting Systems WinEDS 3.1.012 (NASED certified version that was currently in-use by the jurisdiction) and WinEDS 4.0 with WinETP.

WinEDS v.4.0 with WinETP and San Francisco RCV was tested with Optech 400-C and Optech Insight Plus optically scanned paper ballots.

This test effort incorporated:

- Development of functional test requirements based upon Sequoia Voting System *Ranked Choice Voting,* Sec 13.102 of Article XIII *City and County of San Francisco Municipal Code 1996 Charter, Instant Runoff Elections* and *California State Law Elections CODE Section 15650-15654;*
- Pre-test source code review of the Extended Services snap-ins and utilities to identify the applicability to the requirements and the extent of testing required;
- A witnessed build and source code escrow of source code previously reviewed by iBeta as part of Sequoia Voting System's federal certification application SEQ0701;
- Development of a test plan detailing functional testing;
- Review and acceptance of the test plan by Sequoia Voting Systems;
- Management of the voting system configurations;
- Development and execution of a set of functional system level test cases;
- Reporting of defects and validation of their resolution; and
- Analysis of results

The execution of the original 12 test cases uncovered a number of discrepancies that were immediately addressed by Sequoia Voting Systems and regression tested by iBeta. The final regression test (re-execution of a full-end-to-end test with the final WinEDS build) was completed without any additional items identified. All defects identified during functional testing are closed. In the opinion of iBeta Quality Assurance, the acceptance requirements identified in Test Report were met.

At the conclusion of the test effort, the RCV snap-in was then submitted to be included as part of the WinEDS 4.0 Extended Services in the federal test campaign (functional tested in the Primary 1 Test Method and corresponding Test Case as documented in this final test report).

7.9.2 Pierce County Washington

The focus of this test effort was to review the modifications to the source code from WinEDS 4.0.108 with AvcEdge 1.2.56.0 to WinEDS 4.0.108 with AvcEdge 1.2.57.0 in accordance with the iBeta Source Code Review Procedure. The modification consisted of 3 lines of code and 5 lines of comments. Due to the small size of this test effort, the test plan was provided in a letter format.

Once the source code review was complete, a witness build of the updated source code was conducted and the build installations provided on CD with a Final Report to the Office of the Washington Secretary of State. All tasks were completed successfully. This test effort had no impact on the federal certification test campaign.

7.9.3 Illinois Board of Elections

The focus of this test effort was functional testing tailored to the design and complexity of software and the type of voting system hardware deployed in Cook County, Illinois (see list of voting devices below for that configuration). The test effort start date was 9 March 2009. A separate test plan was submitted and approved by the Illinois Board of Elections prior to test initiation. The test effort was completed on 11 August 2009 with the approval and acceptance of the Test Report by the Illinois Board of Elections.

The Sequoia Voting System, WinEDS v.4.0: Independent Voting Systems Testing for the State of Illinois Test Plan v1.0 dated 1 May 2009 identified iBeta's approach to independent testing of the Sequoia Voting Systems WinEDS 4.0 for the State of Illinois. The test effort incorporated an Election Management System and three voting devices:

- The WinEDS election management system for ballot preparation and central count functions;
- The *EDGE2plus* touch screen Direct Recording Electronic (DRE) video and audio voter editable ballot devices with a Voter Verified Paper Audit Trail (VVPAT) with accessible ballot inputs for voters with manual dexterity limitations (models CO.3 and CO.4);
- The Optech Insight Plus precinct count optical scanners; and
- The Optech 400-C central count optical scanner, with WinETP.

This Test Case Design provided the complete functional test cases, system level test cases, documentation of the source code escrow (sources, control, and versioning), reporting requirements, document pass/fail criteria, discrepancy reporting requirements, test project status reporting, and project communication.

The Test Report v1.0 dated 11 August 2009 identified the test activities that were conducted to support the Illinois Board of Elections and summarized the functional testing of the Sequoia Voting Systems WinEDS 4.0.141. The purpose of the final test report was to document the scope and detail of the requirements of functional testing of Cook County, Illinois, voting configuration, including an overview of the pretest activities, functional testing and test findings.

This Test Report identified the test activities conducted to support the Illinois Board of Elections and contains:

- Development of functional test requirements based upon Sequoia Voting System functionality and State of Illinois board of elections.
- Pre-test source code review of the applications utilized in the functional test effort;
- Witnessed builds and source code escrow of source code previously reviewed by iBeta as part of Sequoia Voting System's federal certification application SEQ0701;
- Witnessed builds and source code escrow of source code reviewed by iBeta as part of this test effort;
- Development of a test plan detailing functional testing;
- Review and acceptance of the test plan by Sequoia Voting Systems and the Illinois Board of Elections;
- Management of the voting system configurations;
- Development and execution of a set of functional system level test cases;

- Reporting of defects and validation of their resolution; and
- Analysis of results

During the testing effort, iBeta noted a number of *VSS 2002* requirements that were out-of-scope for this State test effort as identified in NOC 2007-03, States may use an EAC accredited laboratory to conduct testing of a sub-set of the requirements. Additionally, there were a number of *VSS 2002* requirements that would not be met in a federal certification test effort and those requirements were marked as 'Reject' in the requirements matrix in Appendix A and traced to Appendix C which contains either the resolution or the mitigation provided by Sequoia within the Final Test Report.

The Illinois State discrepancies were re-tested during the federal test campaign and those discrepancies, once re-verified, were listed in Appendix E and tracked to closure.

7.10 *Appendix J Sequoia Voting Systems Release 4.0 Implementation Statement*

A copy of the Sequoia Voting Systems Release 4.0 implementation statement is provided as an attachment. To view, select **Attachments** in the **View** menu in Adobe.

7.11 *Appendix K – EAC Certification Number & Voting System Configuration*

This report was submitted to the Election Assistance Commission on 8 September 2010. It is pending their acceptance. No certification number has been issued. When iBeta receives notification that the report is accepted, a revised version of the report will be issued. The Certification number will appear here and on the Title page. Any other revisions will be noted in the version history

This Certification is for the Voting System Hardware and Software configuration(s) listed in section 3.1.

PRO V&V
VERIFICATION VALIDATION

6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Phone (256)713-1111
Fax (256)713-1112

Dominion Democracy Suite 5.10-A Software Test Report for the State of California

Version: 00

Date: 06/25/2020

U.S. Election Assistance Commission
VSTL

EAC Lab Code 1501

NVLAP®

NVLAP LAB CODE 200908-0

SIGNATURES

Approved by: Michael L. Walker — 06/25/2020

Michael Walker, VSTL Project Manager — Date

Approved by: Wendy Owens — 06/25/2020

Wendy Owens, VSTL Program Manager — Date

REVISIONS

Revision	Description	Date
00	Final Report-Initial Release	06/25/2020

TABLE OF CONTENTS

1.0 INTRODUCTION

The purpose of this Test Report is to document the results of D-Suite 5.10-A System Level Image Creation. The scope of the evaluation included performing a source code review of the submitted modified source code, generating trusted builds, installing the trusted builds for the Windows-based components and creating trusted images of all Windows-based components.

1.1 References

The documents listed below were utilized in the development of this Test Report:

- California Voting System Standards (CVSS)
- Election Assistance Commission Testing and Certification Program Manual, Version 2.0
- Election Assistance Commission Voting System Test Laboratory Program Manual, Version 2.0
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-2016, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated July 2016
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008
- United States 107th Congress Help America Vote Act (HAVA) of 2002 (Public Law 107-252), dated October 2002
- Pro V&V, Inc. Quality Assurance Manual, Version 7.0
- D-Suite 5.10-A Technical Documents *(A listing of the TDP documents submitted for this test campaign is listed in Table 3.1 of this Test Report)*

1.2 Terms and Abbreviations

The terms and abbreviations applicable to the development of this Test Report are listed below:
"COTS" – Commercial-Off-The-Shelf

"CVSS" – California Voting System Standards

"D-Suite" – Democracy Suite

"EAC" – United States Election Assistance Commission

"EMS" – Election Management System

"ICC" – ImageCast Central

"ICE" – ImageCast Evolution

"ICX" – ImageCast X

"ICP2" – ImageCast Precinct 2

"ICVA" – ImageCast Voter Activation

"MBP" – Mobile Ballot Printing

"VSTL" – Voting System Test Laboratory

1.3 Background

The D-Suite 5.10-A system is a modification baselined from the current California-approved D-Suite 5.10 system configuration. The baseline system for the source code review report is D-Suite 5.10, which has been previously approved by the state.

1.4 System Overview

The Democracy Suite 5.10-A Voting System is a paper-based optical scan voting system consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC) ballot scanner, the ImageCast Precinct 2 (ICP2) precinct count tabulator, ImageCast Evolution (ICE) precinct count tabulator, ImageCast Voter Activation (ICVA), Mobile Ballot Printing (MBP), and ImageCast X (ICX) BMD ballot marking device.

1.5 Description of Component Code

The table below provides the component lines of code for D-Suite 5.10-A.

Table 1-1 Democracy Suite 5.10-A Component Lines of Code

Component	Language/s	Lines of Code	Standard
EMS*	C#	1,721,537	SD_CSharp_AutomatedCodeReview_5.10_A.pdf
ICP2	C/C++	486,907	SD_CplusPlus_CodingStandard_5.10_A.pdf
ICX	Java	224,307	SD_DVSJavaCodingStandards_5.10_A.pdf
ICE	C/C++	852,980	SD_CplusPlus_CodingStandard_5.10_A.pdf
ICC	C/C++	231,903	SD_CplusPlus_CodingStandard_5.10_A.pdf
ADJ	C#	200,913	SD_Csharp_AutomatedCodeReview_5.10_A.pdf

**Note: EMS Includes ICVA and MBP.*

1.6 Scope of Testing

Pro V&V performed an evaluation of the results from the previous test campaign along with the changes made to the system to determine the scope of testing required for the submitted modification. It was determined the tasks listed below would be required to verify successful system implementation of all modifications:

- Source Code Review, Trusted Build, and Build Document Review

- Installation of the Trusted Builds of the Windows-based Components
- System Level Image Creation

1.7 Testing Overview

The evaluation of D-Suite 5.10-A addressed each of the following test goals in the following manner:

Table 1-2: Testing Overview

Test Goal	Description
Perform Source Code Review, Compliance/Trusted Builds, and Documentation Review	Trusted Builds were generated during the test campaign. The source code submitted by Dominion was reviewed by Pro V&V to the California Voting System Standards (CVSS). The reviewed code was successfully built using the submitted COTS and third-party software products. Additionally, build documentation was reviewed.
Installation of the Trusted Builds of the Windows-based Components	Windows-based components were installed onto the respective workstations to ensure that all workstations were set up correctly.
Perform System Level Image Creation	Trusted images were created during the campaign for California to load to ensure that the integrity of the system.

2.0 TEST CANDIDATE

The Democracy Suite 5.10-A Voting System is a paper-based optical scan voting system that includes proprietary software and firmware. D-Suite 5.10-A consists of the following major components:

- Election Management System (EMS) 5.10.50.83
  - Election Event Designer 5.10.50.83
  - Results Tally Reporting 5.10.50.83
  - Audio Studio 5.10.50.83
  - File System Service 5.10.50.83
  - Data Center Manager 5.10.50.83

- Application Server 5.10.50.85
- Election Data Translator 5.10.50.83
- EMS Service 5.10.50.83
- Adjudication Services 5.10.50.10

  Note: EMS APPS component version is 5.10.50.85

- Adjudication Client (ADJ) 5.10.50.12
- ImageCast Central (ICC) ballot scanner 5.10.2.0001
- ImageCast Precinct 2 (ICP2) precinct count tabulator 5.10.5.1
- ImageCast X (ICX) BMD ballot marking device 5.10.12.4
- ImageCast Voter Activation (ICVA) 5.10.50.83
- ImageCast Evolution (ICE) precinct count tabulator 5.10.10.3
- Mobile Ballot Printing (MBP) 5.10.50.83
- Reformatting Workstation

3.0 TEST PROCESS AND RESULTS

The following sections outline the test process that was followed to evaluate the D-Suite 5.10-A System under the scope defined in Section 1.6.

All testing was conducted under the guidance of Pro V&V by personnel verified by Pro V&V to be qualified to perform the testing.

3.1 Summary Findings and Recommendation

Summary findings for this evaluation are detailed in the following sections.

3.1.1 Source Code Review, Trusted Build, and Build Document Review

A source code review was performed to review the submitted source code to the California Voting Systems Standard (CVSS) and the manufacturer-submitted coding standards. Prior to initiating the review, Pro V&V verified that the submitted documentation was sufficient to enable: (1) a review of the source code and (2) Pro V&V to design and conduct tests at every level of the software structure to verify that design specifications and performance guidelines were met.

The source code review was based on the source code changes made since the previous system was certified. Both manual and automated review techniques were used per EAC approved procedures. A combination of Automated Source Code Review (utilizing the StyleCop statistical code analysis tool) and Manual Source Code Review methods were used to review the changes in the source code. In addition, 10% of the source code comments were manually reviewed.

The Source Code Review included a Trusted Build of the submitted source code. To perform the Trusted Build, Dominion-submitted source code, COTS, and Third-Party software products were inspected and combined to create the executable code. Additionally, during the performance of the Trusted Build, the build documentation was reviewed.

Summary Findings

Pro V&V performed a differential analysis of the EMS 5.10.50.85 source code against the baseline EMS 5.10.50.83 and noted only two source code files were changed (DocumentToHtmlConverter.cs and HtmlTagAttributes.cs), which are described below.

- DocumentToHtmlConverter.cs.

  This file contains logic for converting the text documents from the EMS database that contain the ballot information (headers, contest, candidates, etc.) into the Standard HTML format required by the ICX to display the information. A few methods were changed to update the logic of which HTML elements are used and also how they are put together to create the HTML file.

- HtmlTagAttributes.cs.

  This file contains the constant strings (static definitions) of the HTML elements that are being used. This file was changed due to different notation for the Standard HTML file required by the ICX.

The changes to these two files only affect the EMS Application Server (APPS) component. The affected functionality is the election file generation for the ICX. This is the process where the EMS creates the election definition files for the ICX machines. More specifically, it's in the process of the creation of the HTML documents used by the ICX to display content.

The review of the source code included:

- A review for adherence to the applicable standards in Sections 5 and 7 of the CVSS
- A review for adherence to other applicable coding format conventions and standards including best practices for the coding language used
- An evaluation as to whether the system is designed in a way that allows meaningful analysis, including:
  - Whether the architecture and code is amenable to an external review

- Whether code analysis tools can be usefully applied

Security considerations reviewed against the code included an analysis of error exception handling. Pro V&V considered the modifications to be minor in nature; therefore, an in-depth security review was not required as part of the scope of the evaluation.

3.1.2 Installation of the Trusted Builds of the Windows-based Components

Installation of the Trusted Builds for the Windows-based components included the installation of all Windows-based components onto their respective workstations. Installation documentation review was performed to ensure that all required equipment and software were current and installed correctly.

Summary Findings

Build documents and installation guides utilized during the evaluation are listed below.

Table 3-1: D-Suite 5.10-A TDP Documents

Description	Version
Build Documents	
Democracy Suite ImageCast Evolution Firmware Build Prerequisites Setup and Installation	5.10-A::1
Democracy Suite ImageCast Precinct 2 Build Environment and Prerequisite Setup, Firmware Build and Installation	5.10-A::4
Democracy Suite ImageCast X Build	5.10-A::5
Democracy Suite Windows Build Document	5.10-A::16
Installation Guides	
Democracy Suite EMS Client Workstation Installation and Configuration Procedure	5.10-A::1
Democracy Suite EMS Standard System Installation and Configuration Procedure	5.10-A::1
Democracy Suite ImageCast Central Installation and Configuration Procedures	5.10-A::3
Supplemental Documents	
Appendix to 5.10-A Integrated Build Document	---

3.1.3 System Level Image Creation

System Level Image Creation included the production of creating Windows-based images that could be reloaded onto new workstations to verify the integrity of the systems.

Summary Findings

Once all setup was complete, the procedures detailed in the submitted documentation were followed to make trusted images of all Windows-based systems.

4.0 SUMMARY

Based on the evaluation performed and the results obtained, the D-Suite 5.10-A successfully completed the evaluation with no issues noted. For each source code base submitted (EMS/ICVA/MBP, ICP2, ICX, ICE, ICC, and ADJ) there were no source code requirements found to be at issue with the source code reviewed; as a result, no discrepancies were noted. Additionally, there were no vulnerabilities found within the reviewed source code; therefore, no findings were written against any of the source code bases.

Trusted builds, source code, and images were provided to the State of California per Dominion's request. Along with the trusted build and images, hash values contained in the Hash_Cert_Folder.txt file were archived in the media that Pro V&V provided to the State of California.

As directed by the California Secretary of State Office, this software evaluation report does not include any recommendation as to whether or not the system should be approved.

I'm guessing the old Holocaust office may be currently "held over the head" of A.L.H. as collateral to push her. You may find this aligns with me saying to return her property, if you reviewed my exhibits.

jt4590@protonmail.com

From: ThorfinThunder | GoldGrenade <jt4590@protonmail.com>
Sent: Wednesday, November 1, 2023 11:56 PM
Subject: Re: Opinion

https://youtu.be/xMsiFKjJcFo?si=_lPYG-l_MbMV26gn

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice

-------- Original Message --------
On Nov 1, 2023, 11:53 PM, ThorfinThunder | GoldGrenade < jt4590@protonmail.com> wrote:
"I didn't hear him lay out a plan... I didn't hear the FBI Director lay out a plan..."

In my opinion, there's may be reason, since it was just reported that some of the staffers under Mayorkas may be celebrating deaths of Jews, or at least arrival of HAMAS terrorists via parachute... I don't think you could give any plan there in the public eye during that.

Sir, I have Jewish heritage, and truly, this is a tragedy and a problem currently. I made a report in my case, and the attorney against us made illegal actions, recorded in public record just after the September 11th attacks.

It could be coincidental, but it is concerning, and even after he found he was involving himself in a conspiracy, he continued to attempt to take my rights: Ronald J. Moore.

Despite knowing we were threatened and that his clients were not threatened and perjured, he continued, and it is concerning.

Sincerely,
Jon F. D. Turpin, Pro Se, Pro Hac Vice

For clarity since I saw reports referenced publicly after hearing about HAMAS...
I'm not an "islamaphobe" either, hate portrayed by others, against any group based upon how we were born and/or our heritage is such a tragedy.

Arnold Schwarzenegger has a moving video recently urging against ideologies based upon hatred, and I affirm his opinion.

Gmail

Jon F Turpin <jt4590@gmail.com>

Ronald S. Reese admitted that Dave Holwager contacted him, which causes a tie-in to Colorado. So, maybe the following exhibits can be requested?

Reminder: New Address Update for David Richard Holwager

1 message

Whitepages <reply@email-whitepages.com> Mon, Oct 9, 2023 at 4:13 PM
Reply-To: Whitepages <reply-fe8c1570716c01747d-545_HTML-99270595-100009525-16427@email-whitepages.com>
To: jt4590@gmail.com

Whitepages

Don't miss the recent changes to David Richard Holwager's report

NEW

David Richard Holwager

Aurora, CO

NEW
Addresses

See what's new

Stop monitoring

Stay up to date on the people you know

DISTRICT COURT, DENVER COUNTY, COLORADO 1437 Bannock Street Denver, CO 80202	DATE FILED: September 17, 2021 8:12 PM FILING ID: E9E5DD591D201 CASE NUMBER: 2020CV34319
ERIC COOMER, Ph.D., Plaintiff vs. DONALD J. TRUMP FOR PRESIDENT, INC., et al., Defendants	▲ COURT USE ONLY ▲
Attorneys for Plaintiff Charles J. Cain, No. 51020 ccain@cstrial.com Steve Skarnulis, No. 21PHV6401 skarnulis@cstrial.com Bradley A. Kloewer, No. 50565 bkloewer@cstrial.com Zachary H. Bowman, No. 21PHV6676 zbowman@cstrial.com **CAIN & SKARNULIS PLLC** P. O. Box 1064 Salida, Colorado 81201 719-530-3011/512-477-5011 (Fax) Thomas M. Rogers III, No. 28809 trey@rklawpc.com Mark Grueskin, No. 14621 mark@rklawpc.com Andrew E. Ho, No. 40381 andrew@rklawpc.com RechtKornfeld PC 1600 Stout Street, Suite 1400 Denver, Colorado 80202 303-573-1900/303-446-9400 (Fax)	Case Number: 2020cv034319 Division Courtroom: 409
EXHIBIT E-1	

DISTRICT COURT, CITY AND COUNTY OF DENVER
STATE OF COLORADO
1437 Bannock Street
Denver, CO 80202

^ COURT USE ONLY ^

ERIC COOMER, Ph.D.,
Plaintiff,

Case Number 20CV34319

Courtroom 409

vs.
DONALD J. TRUMP FOR PRESIDENT, INC., SIDNEY POWELL, SIDNEY POWELL, P.C., RUDOLPH GIULIANI, JOSEPH OLTMANN, FEC UNITED, SHUFFLING MADNESS MEDIA, INC., dba CONSERVATIVE DAILY, JAMES HOFT, TGP COMMUNICATIONS LLC, dba THE GATEWAY PUNDIT, MICHELLE MALKIN, ERIC METAXAS, CHANEL RION, HERRING NETWORKS, INC., dba ONE AMERICA NEWS NETWORK, and NEWSMAX MEDIAN, INC.,
Defendants.

VIDEO-RECORDED REMOTE DEPOSITION OF MICHELLE MALKIN

July 27, 2021

REMOTE APPEARANCES:

FOR THE PLAINTIFF:

CHARLES A. CAIN, ESQ.
STEVE SKARNULIS, ESQ.
BRAD KLOEWER, ESQ.
Cain & Skarnulis PLLC
P.O. Box 1064
Salida, Colorado 81201
Telephone: 719-530-3011
Email: ccain@cstrial.com
skarnulis@cstrial.com
bkloewer@cstrial.com

THOMAS M. ROGERS III (TREY), ESQ.
Recht Kornfleld, PC
1600 Stout Street, Suite 100
Denver, Colorado 80202
Telephone: 303-573-1900
Email: trey@rklawpc.com

DISTRICT COURT, DENVER COUNTY, COLORADO 1437 Bannock Street Denver, CO 80202	DATE FILED: September 17, 2021 8:12 PM FILING ID: E9E5DD591D201 CASE NUMBER: 2020CV34319
ERIC COOMER, Ph.D., Plaintiff vs. DONALD J. TRUMP FOR PRESIDENT, INC., et al., Defendants	▲ COURT USE ONLY ▲
Attorneys for Plaintiff Charles J. Cain, No. 51020 ccain@cstrial.com Steve Skarnulis, No. 21PHV6401 skarnulis@cstrial.com Bradley A. Kloewer, No. 50565 bkloewer@cstrial.com Zachary H. Bowman, No. 21PHV6676 zbowman@cstrial.com **CAIN & SKARNULIS PLLC** P. O. Box 1064 Salida, Colorado 81201 719-530-3011/512-477-5011 (Fax) Thomas M. Rogers III, No. 28809 trey@rklawpc.com Mark Grueskin, No. 14621 mark@rklawpc.com Andrew E. Ho, No. 40381 andrew@rklawpc.com RechtKornfeld PC 1600 Stout Street, Suite 1400 Denver, Colorado 80202 303-573-1900/303-446-9400 (Fax)	Case Number: 2020cv034319 Division Courtroom: 409
EXHIBIT F-1	

DISTRICT COURT, CITY AND COUNTY OF DENVER
STATE OF COLORADO
1437 Bannock Street
Denver, CO 80202

^ COURT USE ONLY ^

ERIC COOMER, Ph.D.,
Plaintiff,

Case Number 20CV34319

Courtroom 409

vs.
DONALD J. TRUMP FOR PRESIDENT, INC., SIDNEY POWELL, SIDNEY POWELL, P.C., RUDOLPH GIULIANI, JOSEPH OLTMANN, FEC UNITED, SHUFFLING MADNESS MEDIA, INC., dba CONSERVATIVE DAILY, JAMES HOFT, TGP COMMUNICATIONS LLC, dba THE GATEWAY PUNDIT, MICHELLE MALKIN, ERIC METAXAS, CHANEL RION, HERRING NETWORKS, INC. dba ONE AMERICA NEWS NETWORK, and NEWSMAX MEDIA, INC.,
Defendants.

VIDEO-RECORDED REMOTE DEPOSITION OF JAMES HOFT, individually and as authorized representative of TGP COMMUNICATIONS, LLC, dba THE GATEWAY PUNDIT

August 10, 2021

REMOTE APPEARANCES:
FOR THE PLAINTIFF:
STEVE SKARNULIS, ESQ.
BRAD KLOEWER, ESQ.
Cain & Skarnulis PLLC
P.O. Box 1064
Salida, Colorado 81201
Telephone: 719-530-3011
Email: skarnulis@cstrial.com
bkloewer@cstrial.com